NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

HACKING YOUR RIDE: IS WEB 2.0 CREATING VULNERABILITIES TO SURFACE TRANSPORTATION?

by

Cedric Novenario

September 2016

Thesis Advisor: Wayne Porter
Second Reader: Robert Schroeder

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE HACKING YOUR RIDE: IS WEB 2.0 CREATING VULNERABILITIES TO SURFACE TRANSPORTATION?		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Cedric Novenario			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The purpose of this thesis is to determine the threats that social media and social navigation (SMSN) pose to the surface transportation system. The research catalogs the types of threats and SMSN's vulnerabilities, and uncovers terrorists' malign use of social media for intelligence gathering. Academic researchers have already discovered threats in social navigation platforms such as Waze and Google Maps; Sybil and man-in-the-middle attacks allow malicious actors to create traffic congestion and alternate vehicle routing. While this has not yet caused an attributable security concern to the vehicle surface transportation system, in the hands of malicious actors, these vulnerabilities could be exploited to orchestrate an attack that devastates infrastructure and risks human lives.

14. SUBJECT TERMS social media, social navigation, Web 2.0, surface transportation security, vehicle transportation security, Waze, Google Maps, traffic congestion, traffic management security, transportation security vulnerabilities, transportation security threats			**15. NUMBER OF PAGES** 91
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

HACKING YOUR RIDE: IS WEB 2.0 CREATING VULNERABILITIES TO SURFACE TRANSPORTATION?

Cedric Novenario
Transportation Services Manager, City of Los Altos, CA
B.S., San Jose State University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2016**

Approved by: Wayne Porter, Ph.D.
Thesis Advisor

Robert Schroeder
Second Reader

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to determine the threats that social media and social navigation (SMSN) pose to the surface transportation system. The research catalogs the types of threats and SMSN's vulnerabilities, and uncovers terrorists' malign use of social media for intelligence gathering. Academic researchers have already discovered threats in social navigation platforms such as Waze and Google Maps; Sybil and man-in-the-middle attacks allow malicious actors to create traffic congestion and alternate vehicle routing. While this has not yet caused an attributable security concern to the vehicle surface transportation system, in the hands of malicious actors, these vulnerabilities could be exploited to orchestrate an attack that devastates infrastructure and risks human lives.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

app	mobile application
CalTrans	California Department of Transportation
FEMA	Federal Emergency Management Agency
GPS	Global Positioning System
IED	improvised explosive device
ISIS	Islamic State of Iraq and Syria
ITS	intelligent transportation systems
SMSN	social media and social navigation
SNA	social network analysis
TPA	Technosocial Predictive Analysis
TSA	Transportation Security Administration

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Traffic congestion during commuting hours (7:00 A.M. to 9:00 A.M. and 4:00 P.M. to 6:00 P.M.) is as much a guarantee as death and taxes. Sitting in traffic gridlock consumes valuable free time, adds pollutants to the air, and reduces overall quality of life.[1] Developers from the mobile application (app) world have created apps such as Waze and Google Maps that not only link traffic navigation software to near-real-time Global Positioning System (GPS) updates, but also to live, crowdsourced traffic information provided by fellow commuters; this information is designed to reduce traffic congestion and help commuters avoid traffic snarls or obstacles.[2] Mobile apps like Waze and Google Maps can be considered social navigation.

Unfortunately, there is little research regarding the impact of social media and social navigation (SMSN) specific to surface transportation security. Likewise, research evaluating the influence of SMSN on human or "user" behavior and the associated vulnerabilities to the transportation system is also lacking. Perhaps the impact of SMSN apps on surface transportation has not been explored in more depth because the focus has primarily been on transportation infrastructure—bridges, overpasses, highways—and transportation control systems. However, SMSN apps should be considered an integral part of the surface transportation system; the information that users contribute and distribute influences human behavior and the resulting behavior of the transportation system itself.

This thesis catalogs malign SMSN tools, tactics, and techniques that pose a security risk to surface transportation. It is hoped that this analysis may lead to a heuristic inquiry that could expose malign activities before they present a threat to the surface transportation system.

To address the threats that SMSN pose to the surface transportation system, this thesis provides a qualitative analysis of the system's specific SMSN-related

[1] This information is based on my experience as a traffic and transportation engineer.

[2] "Crowdsourced Traffic Apps: Saving Commuters from Traffic Jam Torture," *Scratch,* February 10, 2015, http://www.scratchmarketing.com/crowdsourced-traffic-apps/.

vulnerabilities by conducting a thorough and systematic review of academic journals, books, white papers, websites, and open-source information from popular social media and social navigation sites such as Twitter, Facebook, and Waze. Vulnerabilities/threats are cataloged by existing and known vulnerabilities, and potential malign uses of SMSN tools and tactics that have not yet been attempted. The data is further grouped into three categories: SMSN manipulation, social navigation manipulation, and use of SMSN for intelligence.

No conclusive evidence was found that social media is a direct threat to the surface transportation system. However, there is implied potential for social media's exploitation by terrorist groups and individuals. Of most concern is that these groups or individuals will disseminate false information to control the narrative or behavior of social groups, or that they will use legitimate information as a source of intelligence. For example, when Twitter users post their sentiments regarding traffic conditions, malicious actors can use this tactical knowledge to attack the surface transportation system.

Researchers have discovered that social navigation applications, such as Waze and Google Maps, are vulnerable to Sybil and man-in-the-middle attacks.[3] A Sybil attack exploits trust vulnerabilities in web and mobile application platforms that depend on user interaction and crowdsourced information by disregarding terms of use agreements (which preclude the deliberate introduction of false information) through imposter identities.[4] These imposter identities can present false or alternative information that incorrectly guides users in a manner desired by the malicious actor. Waze, for example, will suggest alternate travel routes should the targeted route have a comparatively longer travel time.[5] Should the Sybil attack trigger traffic congestion, malicious actors can lure unsuspecting motorists into "kill boxes" to orchestrate an attack. While social media apps

[3] Gang Wang et al., "Defending against Sybil Devices in Crowdsourced Mapping Services," paper presented at MobiSys '16, Singapore, June 25–30, 2016; Meital Ben Sinai et al., *Exploiting Social Navigation* (Haifa, Israel: The Technion, 2014); Tobias Jeske, "Floating Car Data from Smartphones—What Google and Waze Know about You and How Hackers Can Control Traffic," paper presented at Black Hat Europe, Amsterdam, March 12–15, 2013.

[4] "Terms of Use," Waze, accessed July 14, 2016, https://www.waze.com/legal/tos; "Google Maps/Google Earth Additional Terms of Service," Google, December 17, 2015, https://www.google.com/intl/ALL/help/terms_maps.html.

[5] Wang et al., "Defending against Sybil Devices," 4

such as Waze and Google Maps are not typical platforms for terrorism, surface transportation does represent a soft target with high potential for large-scale casualties.[6] A Sybil attack on one of these apps could provide a new target vector for terrorists, rendering highway infrastructure or passenger vehicles an attractive soft target. This would be especially devastating in the United States, where motor vehicles are the predominant mode of travel, with potential attacks impacting tens of millions of urban commuters daily.[7]

In the near future, terrorist or criminal Sybil attacks could target autonomous vehicles, which are expected to communicate with transportation infrastructure to ensure efficient and safe traffic flow.[8] A Sybil or man-in-the-middle attack on the traffic infrastructure and/or vehicular network could communicate false vehicle characteristic information or false traffic infrastructure information, causing vehicle conflicts and accidents at intersections. Homeland security professionals must be prepared to address these vulnerabilities as the future of vehicle surface transportation becomes an increasingly interconnected network.

---

[6] Brian Michael Jenkins and Bruce R. Butterworth, *Troubling Trends in Terrorism and Attacks on Surface Transportation: The Outlook is Grim, but People Still Have a Great Deal of Control* (San Jose, CA: Mineta Transportation Institute, 2015), 2.

[7] Tom Huddleston, Jr. "These U.S. Cities Have the Worst Commute Times," *Fortune*, March 3, 2016, http://fortune.com/2016/03/03/us-cities-average-commute-time/.

[8] Rupesh Gunturu, "Survey of Sybil Attacks in Social Networks," Cornell University Library, accessed April 15, 2016, http://arxiv.org/pdf/1504.05522v1.pdf; "Vehicle-to-Infrastructure (V2I) Communications for Safety," U.S. Department of Transportation, accessed July 12, 2016, http://www.its.dot.gov/factsheets/v2isafety_factsheet.htm.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my committee, Dr. Wayne Porter and Robert Schroeder, for their guidance and encouragement during the development of my thesis. I really enjoyed working with you both, and I am sincerely appreciative that you supported the vision of my thesis and saw a value in its pursuit. I am grateful to Dr. Lauren Wollman for her early guidance in our research classes. You helped me set a foundation for my thesis research.

To my former city manager, Marcia Somers; Police Chief Tuck Younis; Public Works Director Susanna Chan; and my staff, Kathy Small and Daniel Varela, of the City of Los Altos: Thank you for supporting me during the program and allowing me to expand my horizons. I am grateful to you all.

To my classmates in Cohort 1501/1502: I am reminded every in-residence session how lucky I am to be around you all. You all have made a positive impact on my life and I will cherish that forever. Thank you.

To my son: Thank you for telling me I look too serious when studying and making me laugh on those early Saturday mornings. You remind me that life should also be fun.

To my daughter: You are an example of hope. You remind me to live in the moment. You inspire me to be a better dad. Thank you.

To my wife: I am thankful for your patience and encouragement during my journey through this program. You kept me focused when I thought I could not finish and pointed out that I belong in the program. Between your doctorate program, CHDS, and our daughter's home schooling, it was a very stressful year and a half, but we made it. Thank you for pushing me to new heights.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Traffic congestion during commuting hours (7:00 A.M. to 9:00 A.M. and 4:00 P.M. to 6:00 P.M.) is as much a guarantee as death and taxes. Sitting in gridlock consumes valuable free time, adds pollutants to the air, and reduces overall quality of life.[1] So, how do everyday commuters avoid sitting in traffic for several hours? Fortunately, there have been advances in Web 2.0 technology to help ease commuters' frustration. Developers from the mobile application (app) world have created apps such as Waze and Google Maps that not only link traffic navigation software to near-real-time Global Positioning System (GPS) updates, but also to live, crowdsourced traffic information provided by fellow commuters; this information is designed to reduce traffic congestion and help commuters avoid traffic snarls or obstacles.[2] Navigation apps like Waze have become popular because they offer commuters alternative transportation choices. It is estimated that "over 50 million active users log into Waze monthly," which is a testament to the popularity and utility of navigation apps.[3] Waze, in particular, is actively looking to partner with state and local transportation agencies in the spirit of sharing transportation data to reach as many road users as possible.[4] The imminent partnership is evidence that the growing navigation app market is becoming part of the surface transportation system.

Social networks and social media have proven to be effective tools for influencing human behavior.[5] A simple Google search of "social media's influence on human

---

[1] This information is based on my experience as a traffic and transportation engineer.

[2] "Crowdsourced Traffic Apps: Saving commuters from traffic jam torture," Scratch, February 10, 2015, http://www.scratchmarketing.com/crowdsourced-traffic-apps/.

[3] Sarah Perez, "Navigation App Waze Gets a Huge Redesign-Now Less Cluttered, but Still Needs Improvement," Tech Crunch, last modified October 19, 2015, http://techcrunch.com/2015/10/19/navigation-app-waze-gets-a-huge-redesign-now-less-cluttered-but-still-needs-improvement/#.zpel8b:KuBe.

[4] Neal Underleider, "Waze Is Driving into City Hall," Fast Company, last modified April 15, 2015, http://www.fastcompany.com/3045080/waze-is-driving-into-city-hall.

[5] Dick Dahl, "Experts Explore How Social Networks Can Influence Behavior and Decision Making," video, Harvard Law School, February 15, 2013, http://today.law.harvard.edu/experts-explore-how-social-networks-can-influence-behavior-and-decision-making-video/.

behavior" yields pages of blogs and scholarly articles analyzing this phenomenon. The importance of social networks and social media have long been recognized and exploited by terrorist groups such as the Islamic State of Iraq and Syria (ISIS). A report by Lieutenant Commander Nathan K. Schneider of the U.S. Navy describes the proficiency with which ISIS uses social media:

> Social media integration has been pivotal in ISIS's success at the operational level of war in Iraq and Syria. Demonstrating a keen ability to achieve a unity of effort, ISIS has been successful at synchronizing its social media efforts with its military operations in Iraq.[6]

Further, ISIS capitalizes on trending news information by co-opting trending hashtags (the hash character or pound sign preceding a word).[7] Co-opting hashtags thrusts ISIS to the front of news media and extends their terrorist message to the masses.[8]

Unfortunately, research regarding the impact of social media and social navigation (SMSN) specific to surface transportation security is minimal. Likewise, research evaluating the influence of SMSN on human or "user" behavior and the resulting vulnerabilities to the transportation system is also lacking. Thus, our understanding of the threats SMSN pose to the surface transportation system is limited.

While technological improvements such as social navigation apps can improve efficiencies in the surface transportation system, their malicious use could result in immediate repercussions, such as increased traffic congestion, increased traffic collisions, or deliberate rerouting of traffic for criminal or terrorism purposes. At the extreme, social navigation apps could provide intelligence to coordinate a vehicle-borne explosion, which could destroy city infrastructure and cause mass casualties.

---

[6] Nathan K. Schneider, *ISIS and Social Media—The Combatant Commander's Guide to Countering ISIS's Social Media Campaign* (Newport, RI: Naval War College, 2015), 13.

[7] Alexander Trowbridge, "ISIS Swiping Hashtags as Part of Propaganda Efforts," CBSNews, August 26, 2014, http://www.cbsnews.com/news/isis-hijacks-unrelated-hashtags-in-attempt-to-spread-message/.

[8] Ibid.

1. Not a New Concern

Malicious exploitation of social navigation applications is not a new concern. In 2015, Malaysian politician Datuk Raime Ungii, in a statement to the Malaysian parliament, expressed, "Terrorist groups may easily be able to access our location. They may monitor the public and important figures through it."[9] He goes on to assert that, "We need to know the reach of these apps and I will continue to ask questions when there is space for it in [lower parliament]."[10]

In 2014, students from the Technion University in Israel created false Waze user accounts, which they used to manipulate and plant false information in order to influence the movement of traffic and create gridlock throughout Technion.[11] This is an example of how navigation apps can be deliberately exploited to affect social behavior. While the app was manipulated for a research project and not with malicious intent, the students' work uncovered vulnerabilities to the surface transportation system. Aware of this Waze hack project, author and former staff director of the U.S. Senate Foreign Relations Committee, Dr. Stephen Bryen, expressed his concerns on his *Technology and Security* blog:

> If Waze can be faked, it can be used to set traps that could prove fatal. In Israel it is a genuine threat-risk. For example, Hamas and Hezbollah, not to mention the Syrian Electronic Army and its equivalent in Iran, and probably Isis too, can spoof an app like Waze and use it to lead both military, police and private citizens into ambushes.[12]

Similar concerns exist in the United States, where motor vehicle use far exceeds public transportation use.[13] Waze is one of the most popular traffic navigation

---

[9] Veena Babulal, "Apps Like Waze and Google Map Risk national security with rise of IS?," *New Straits Times Online*, November 27, 2015, http://www.nst.com.my/news/2015/11/114220/apps-waze-and-google-map-risk-national-security-rise.

[10] Ibid.

[11] David Greenway, "Students Fake a Traffic Jam in Waze to Clear Their Route," htxt.africa, accessed July 8, 2015, http://www.htxt.co.za/2014/03/26/students-fake-a-traffic-jam-in-waze-to-clear-their-route/.

[12] Stephen Byren, "Waze, Qalandia and Social Media Danger," *Technology and Security*, March 1, 2016, https://technologysecurity.wordpress.com/2016/03/01/waze-qalandiya-and-social-media-danger/.

[13] Ralph Buehler, "9 Reasons the U.S. Ended up So Much More Car-Dependent Than Europe, *CityLab*, February 4, 2014, http://www.citylab.com/commute/2014/02/9-reasons-us-ended-so-much-more-car-dependent-europe/8226/.

applications, with an estimated 5.5 million users in the United States in 2013.[14] Waze use will only continue to grow as motorists seek routes to circumvent traffic, and thus the opportunity to manipulate users in the United States is also likely to grow.

2. Significance of the Research

Threats to surface transportation infrastructure have long been on the U.S. Department of Homeland Security's mind; surface transportation is one of sixteen sectors under the purview of their authority. The Transportation Security Administration (TSA) is well aware that malicious actors and terrorists can pose a threat to the U.S. highway system.[15] In a threat assessment report, the TSA asserts that the use of improvised explosive devices (IEDs), vehicle-borne IEDs, and explosives on ships or bridges are common and expected terrorist tactics.[16] However, the assessment contains only a brief description of cyber threats to the transportation system, despite acknowledging that Al Qaeda and other groups may have the ability to wreak havoc on supervisory control and data acquisition systems used to remotely operate vital infrastructure.[17]

Researchers Pamela Murray-Tuite and Xiang Fe have examined risks to the transportation network using attacker-defender analysis.[18] They analyzed several potential targets—ranging from government facilities, bridges, highways, shopping malls, and office buildings—and the impact that disabling one or more targets would have on the supporting transportation network. Murray-Tuite and Fe's examined targets are considered traditional transportation infrastructure; what they did not consider are the potential security implications of traffic navigation apps.

---

[14] Shaul Zohar, "Report—Users—WAZE—2013—United States, Europe, Asia & Latin America," Evolita, September 18, 2014, http://alpha.evolita.com/Research/Subject/WAZE-Users-Europe-Asia-Latin-America-United-States-Y2013.

[15] Alan Hickson, *Terrorist Threat to U.S. Highway Systems* (Washington, DC: Department of Homeland Security, Transportation Security Administration, 2006), 1–2.

[16] Hickson, *Terrorist Threat to U.S. Highway Systems*, 1–2.

[17] Ibid.

[18] Pamela Murray-Tuite and Xiang Fe, "A Methodology for Assessing Transportation Network Terrorism Risk with Attacker-Defender Interactions," *Computer-Aided Civil Engineering* 25, no. 6 (August 2010): 396–410.

For the 2011 IEEE Symposium on Computers and Communications, a group of researchers reviewed vulnerabilities to transportation network links and the effects of a possible attack.[19] The researchers examined motorists' travel times, and the economic impacts of motorists using alternate routes to avoid a failed transportation network link. Their study also attempted to rank the importance of transportation links; in the event of a link failure due to a natural disaster or other catastrophic event, this ranking system can help transportation planners determine which critical transportation links are needed to restore operations or to make the transportation system more resilient. Again, however, vulnerabilities related to traffic navigational apps were not examined. Future analysis of transportation network or infrastructure security should consider these apps because they have become integral to the operation of surface transportation.

Further, an article for TechTarget points out that computerized traffic signal systems are vulnerable to cyberattacks.[20] The TechTarget authors claim that about two-thirds of transportation security practitioners are not prepared for cyberattacks on computerized elements of the transportation system.[21] For example, intelligent transportation systems (ITS) technology incorporates various edge communication devices, such as routers and switches, to transmit data between a transportation management center and the local traffic signal controller.[22] Unfortunately, many ITS systems were designed by traffic and transportation engineers who did not have the foresight to include basic cyber security concepts, such as system encryption.[23] By penetrating a central traffic signal operating system through switches and routers, a malicious actor can alter traffic signal timing patterns that result in accidents or increased traffic congestion.

---

[19] Saleh Ibrahim et al., "An Efficient Heuristic for Estimating Transportation Network Vulnerability," *2011 IEEE Symposium on Computers and Communications (ISCC)*: 1092–1098.

[20] Stephen Barlas et al., "U.S. Critical Infrastructure Security: Highlighting Critical Infrastructure Threats," TechTarget, accessed March 3, 2016, http://searchsecurity.techtarget.com/US-critical-infrastructure-security-Highlighting-critcal-infrastructure-threats.

[21] Ibid.

[22] This is based on my experience as a traffic and transportation engineer.

[23] Ibid.

Perhaps the impact of SMSN apps on surface transportation has not been explored in more depth because the focus has primarily been on transportation infrastructure—bridges, overpasses, highways—and transportation control systems. However, SMSN apps should be considered an integral part of the surface transportation system; the information that users contribute and distribute influences human behavior and the resulting behavior of the transportation system itself. A comprehensive understanding of how SMSN platforms impact transportation security should be pursued as vigorously as any other component of the surface transportation system. Identifying related threats will contribute to the overall foundation of surface transportation security literature.

B. RESEARCH QUESTIONS

This thesis seeks to answer the following broad research question:

What threats do SMSN pose to the surface transportation system?

Two sub-questions, or parts, feed into this broad research question:

A. What are the existing and known vulnerabilities of surface transportation systems to online threats?

B. What are the hypothetical vulnerabilities of these systems?

Part A specifically examines SMSN vulnerabilities that could threaten (U.S.) urban vehicle surface transportation and highway/road infrastructure. This section catalogs both successful and thwarted attacks, hacks, and disruptions to transportation systems. Part B explores potential vulnerabilities/threats/attacks that have not yet been exploited or attempted. These are largely based on vulnerabilities discovered throughout the research process that could disrupt surface transportation systems. Exposing these vulnerabilities could enable the development of a more resilient surface transportation system through enhanced security and awareness. Further, it provides homeland security professionals a foundation from which to prepare solutions.

C. METHODOLOGY

This thesis employs a qualitative methodology that includes a thorough and systematic review of academic journals, books, white papers, and websites. Additional data was gathered from technology-based conferences and blogs. Open-source information from popular social media and social navigation sites such as Twitter, Nextdoor, Waze, Inrix, and Twittraffic also provided information that could be analyzed to reveal vulnerabilities in the transportation system.

The research yields data that exposes vulnerabilities to the transportation system exploited by the use of SMSN. These vulnerabilities can include, but are not limited to, hacking, posting of misinformation, intelligence gathering by malicious actors, and unintended consequences of misuse. Data collected is cataloged by known vulnerabilities and potential malign uses of tools and tactics.

A detailed description of the methodology is included in Chapter III.

D. OVERVIEW OF UPCOMING CHAPTERS

This thesis comprises six chapters. After this chapter (which has provided a thematic introduction and foundation for the research), Chapter II presents a literature review of social media exploitation and social navigation exploitation, and their associated security or operational impacts on the transportation system. Chapter III describes the methods and sources of information from which this research is derived. Chapter IV reveals the information discovered from the research and categorizes the data. Chapter V presents a discussion of the findings and describes discovered trends regarding SMSN threats to the surface transportation system. Chapter VI provides conclusions and suggestions for future research, and answers the research question.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Terrorists' relationship with social media is similar to that of average citizens. Terrorists use social media because it is free, easy to use, and the available information is reliable enough to inform decisions for attack planning.[24] Gabriel Weimann, an expert on terrorists' use of social media, states that terrorists most commonly use social media to spread propaganda, promote radicalization, and recruit new members.[25] Researchers Catherine A. Theohary and John Rollins confirm Weimann's observations, additionally noting that terrorists are developing an ability to circumvent cyber-security measures and conduct cyberattacks.[26] Unequivocally, terrorists are building a capacity to use social media that warrants homeland security professionals' preparation. The remainder of this chapter explores how social media and social navigation platforms can be exploited for malign use. For the purposes of this thesis, malicious actors, terrorists, and dark networks are the groups that are conducting illegal activities.[27]

A. SOCIAL MEDIA EXPLOITATION

The evolution of social media has given malicious actors new territory on which to conduct operations, and has therefore presented security professionals with new challenges.[28] According to Katya Drozdova and Michael Somilov, social media is an optimal operational frontier for terror networks because its speed is tremendously fast, its reach of communication far and numerous, and its methods efficient.[29] Social media also

[24] Paulina Wu, "Impossible to Regulate: Social Media, Terrorists and a Role for the U.N.," *Chicago Journal of International Law* 16, no.1, (2015): 288.

[25] Gabriel Weimann, *New Terrorism and New Media* (Washington, DC: Wilson Center, 2014), 3.

[26] Catherine A. Theohary and John Rollins, *Terrorist Use of the internet: Information Operations in Cyberspace* (CRS Report No. R41674) (Washington, DC: Congressional Research Service, 2011), 5.

[27] Jorg Raab and H. Brinton Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory* 13, no. 4, (2003): 414, doi: 10.1029/jopart/mug029.

[28] Marc Goodman, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do about it* (New York: Knopf Doubleday, 2014), Kindle location 2030–2032.

[29] Katya Drozdova and Michael Samoilov, "Predictive Analysis of Concealed Social Network Activities Based on Communication Technology Choices: Early-Warning Detection of Attack Signals from Terrorist Organizations," *Computational and Mathematical Organization Theory* 16, no. 1 (March 2009): 64–65.

allows terror networks to spread their ideology and messages unimpeded by borders or national laws.[30]

Drozdova and Somilov further contend that the methods of communication among dark networks—direct contact, telephone, or internet—can indicate early warning signs of an impending attack.[31] The article references the traceability and level of covertness based on the communication technology used. For example, low-tech communications such as face-to-face meetings, letters, or signals indicate a higher degree of covertness, while hi-tech communications (e.g., internet, mobile phone, social media) have a higher degree of traceability and vulnerability, but increase task efficiency. The authors applied signals analysis to both low- and hi-tech means of communication and determined that low-tech communications yielded higher indicators of attack precursors.[32] Their research reveals that a first priority of actors in a dark network is to stay undetected. The use of open social media sites for communication can therefore be counterproductive, because information is publicly available and easily obtained. However, because hi-tech communication can facilitate quicker action, dark networks seek to balance covertness and quick action.[33]

Social media has also demonstrated the ability to influence individuals' behavior. In his book, *Linked: How Everything Is Connected to Everything Else and What it Means for Business, Science and Everyday Life*, Albert Lazslo-Barabasi describes the importance of connectors or connections in social networks.[34] Connectors, he explains, can establish trends and bring different groups of people together.[35] Lazslo-Barabasi's concepts apply to social networks on the web as well as traditional social networks. In

---

[30] Yigal Carmon, Steven Stalinsky, "Terrorist Use of U.S. Social Media is a National Security Threat," Forbes, January 30, 2015, http://www.forbes.com/sites/realspin/2015/01/30/terrorist-use-of-u-s-social-media-is-a-national-security-threat/2/

[31] Drozdova and Samoilov, "Predictive Analysis," 63.

[32] Ibid., 85.

[33] Ibid., 64; Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge University Press, 2011), xxvi.

[34] Albert-Laszlo Barabasi, *Linked—How Everything Is Connected to Everything Else and What it Means for Business, Science, and Everyday Life* (New York: Plume-Penguin Group, 2002), 56.

[35] Ibid.

2012, a *Behavior Computing* article confirmed Lazslo-Barabasi's assertion and analyzed social media users' behaviors, as well as the influence users have on the online community.[36] The article suggests that, although behavior resulting from exposure to social media sites varies depending on the purpose of the site, the behaviors' various characteristics and tendencies remain consistent.[37] For example, influential users tend to gravitate toward each other to generate even greater influence over an online community.[38] The article confirms that the use of social media by charismatic actors with well-crafted messages motivates behavior among a network of followers and individuals looking for a place in their society.

Malicious actors can also use social media to impersonate and render false information to control the narrative to their benefit.[39] Controlling the narrative gives malicious actors unchecked power to influence human behavior in their social network. In a policy memo for the Commons Lab at the Wilson Center, Rebecca Goolsby uses the term "Social Cyber Attack" to reflect how a crowd, or social network, can be influenced by "inflammatory information and disinformation."[40] A "Social Cyber Attack" can cause mass confusion and unwarranted agitation among the populous, leading to unmanageable chaos.[41]

On the other hand, terrorists have also used social media to maintain situational awareness during their illegal activities.[42] During the 2008 attacks in Mumbai, terrorists "maintained information superiority," but also obtained "up-to-date situational information by systematically monitoring mainstream media and [social media] web-

---

[36] Nitin Agarwal et al., "Analyzing Behavior of the Influentials Across Social Media," in *Behavior Computing: Modeling Analysis, Mining and Decision*, edited by Longbing Cao and Philip S. Yu, 3–19 (New York: Springer: 2012).

[37] Agarwal et al., "Analyzing Behavior," 4–5.

[38] Ibid., 17.

[39] George Chamales, *Towards Trustworthy Social Media and Crowdsourcing* (Washington, DC: Wilson Center, 2013), 8.

[40] Rebecca Goolsby, *On Cybersecurity, Crowdsourcing, and Social Cyber-Attack* (Washington, DC: Wilson Center, 2013), 3.

[41] Ibid.

[42] Onook Oh, Manish Agrawal, and H. Raghav Rao, "Information Control and Terrorism: Tracking the Mumbai terrorist Attack through Twitter," *Information Systems Front* 13, no. 1 (March 2011): 33.

sites."[43] Overall, Web 2.0 enabled the Mumbai terrorists to stay ahead of authorities, which ultimately strengthened their attacks.[44] Because social media is designed to share and distribute information openly, it is extremely difficult to determine if it is being used for malicious purposes.

Analysts soon realized that it was necessary to leverage social media in order to keep up with terror networks' operations and growth.[45] Thus, new analytical methods with roots in social network analysis (SNA) are currently being evaluated for their predictive capabilities.[46] Technosocial Predictive Analysis (TPA) is one such method, introduced by Maged Kamel Boulos, Antonio Sanfilippo, Courtney Corley, and Steve Wheeler in 2010.[47] In short, TPA is a range of tools and methods that anticipate groups' actions to minimize surprises.[48] Their analysis focused on participants within the techno-society who are more communicative in an online environment.[49] TPA, which can be used to mine data from social networking sites such as Facebook and Twitter, is a multidisciplinary approach that combines physical and human factors to understand the human decision making process. Predicative policing, for instance, is a form of TPA; it takes into account individuals' and groups' social media activities, friendships, past criminal behaviors, and known group boundaries.[50] These factors help law enforcement understand how a person's or group's decision could lead to potential illegal activities, thus enabling law enforcement to proactively address emergent activities.

---

[43] Oh, Agrawal, and Rao, "Information Control and Terrorism," 36.

[44] Ibid., 38.

[45] John Curtis Amble, "Combating Terrorism in the New Media Environment," *Studies in Conflict & Terrorism*, 35, no. 5, (2012): 346, doi: 10.1080/1057610X.2012.666819.

[46] Everton, *Disrupting Dark Networks*.

[47] Maged Kamel Boulos et al., "Social Web Mining and Exploitation for Serious Applications: Technosocial Predictive Analytics and Related Technologies for Public Health, Environmental and National security Surveillance," *Computer Methods and Programs in Biomedicine* 100, no. 1 (October 2010): 16–23, doi: 10.1016/j.cmpb.2010.02.007.

[48] Boulos et al., "Social Web Mining and Exploitation," 19.

[49] Ibid.

[50] John Eligon and Timothy Williams, "Police Program Aims to Pinpoint Those Most Likely to Commit Crimes," *New York Times*, September 24, 2015, http://www.nytimes.com.

Because social media and web data-mining provide open-source, easily accessible information, they can greatly contribute to the overall homeland and national security landscape.[51] SNA complements social media web mining; relationship ties can sometimes be determined through open-source information.[52] Researchers France and Christopher Cheong examined this relationship by analyzing tweets during the 2010–2011 floods in Australia.[53] They were able to identify influential Twitter users during the floods and the users' methods for collecting and distributing information to their followers.[54] Had Australian emergency responders understood this information, they could have used it to preposition response assets, or to disseminate pre-developed emergency response messaging.

The next critical step toward applying SNA to social media is to develop mechanisms or systems that can perform predictive or analytic processes. To do so, Gregory Freeman and Robert Schroeder of the Naval Postgraduate School's Common Operational Research Environment (CORE) Lab evaluated off-the-shelf and government-owned social media analysis software.[55] Their evaluation provided a framework for analyzing social media and the actors who participate in its networks, and suggestions for the tailored application of analytic tools based upon situational criteria. SNA involves gathering and fusing data, and then applying metrics to better understand network behavior; Freeman and Schroeder contend that analysis should combine social network analytic tools (e.g., Ora, UCINET, Pajek) and methods in order to best graphically depict the network and its behavior.[56]

---

[51] Mark Hosenball, "Homeland Security Watches Twitter, Social Media," *Reuters*, January 11, 2012, http://www.reuters.com/article/us-usa-homelandsecurity-websites-idUSTRE80A1RC20120111

[52] France Cheong and Christopher Cheong, "Social Media Data Mining: A Social Network Analysis of Tweets during the 2010–2011 Australian Floods," paper presented at the Pacific Asian Conference on Information Systems, Brisbane, Australia, July 7–11, 2011.

[53] Cheong and Cheong, "Social Media Data Mining."

[54] Ibid., 12.

[55] Gregory Freeman and Robert Schroeder, *Social Media Exploitation: An Assessment* (Monterey, CA: Naval Postgraduate School, 2014).

[56] Freeman and Schroeder, *Social Media Exploitation*, 48.

Researchers have also used social media to assess the impact of natural and manmade disasters on affected communities.[57] Kathryn Blackmond Laskey conducted two controlled experiments: the first experiment simulated a group protest that became violent; in the second experiment, a fictional terrorist group posted threatening messages to a college and county website.[58] The objective of these experiments was to determine if social media is advantageous to responders, decision makers, policy makers, and citizens during or in the aftermath of an emergency.[59] Overall, the study generally demonstrated the benefits of using social media both for those who crowdsourced the information (citizens) and those who used the information to plan and execute tactical response (emergency responders). Emergency responders found that, through social media, citizens provided them enhanced situational awareness; this crowdsourced information helped them make more informed decisions. For the affected citizens, social media provided a real-time assessment of emergency responders' performance during the incident.[60] The study showed that emergency responders developed a certain level of trust in the information provided by social media, and therefore found the use of social media in emergency response valuable.[61] Laskey did not, however, evaluate the effects of malign use of crowdsourced information. If a social media source identifies a false emergency or call for help, pursuing the misinformation can cause disruptions in legitimate response operations, putting citizens and operators in harm's way.[62]

---

[57] Takeshi Sakai et al., "The Possibility of Social Media Analysis for Disaster Management," paper presented at the 2013 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Sendai, Japan, August 26–29, 2013, 238–243.

[58] Kathryn Blackmond Laskey, "Crowdsourced Decision Response for Emergency Responders," paper presented at the 18th International Command and Control Research & Technology Symposium, Alexandria, VA, June 19–21, 2013.

[59] Laskey, "Crowdsourced Decision Response."

[60] Ibid., 8–10.

[61] Ibid., 11.

[62] Bruce R. Lindsay, *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations* (CRS Report No. R41987) (Washington, DC: Congressional Research Service, 2011), 7.

B. SOCIAL NAVIGATION

Can analytical methods help determine if malicious actors are using social media sites to exploit human behavior and compromise transportation security? As mentioned previously, there is limited literature addressing the effects of social media on transportation security. Further research is needed to determine if SNA and geospatial analysis can shed light on security vulnerabilities posed by social navigation apps such as Waze. Analysis could focus on measuring the influence an individual user can have on the behavior of the wider commuter population, and if that user can maliciously influence travel patterns. The students from Technion University in Israel (introduced in Chapter I) have provided a good start. By creating impostor accounts, the students were able to re-route commuters using algorithms that programmed false GPS locations, false crowdsourced information, and false traffic congestion on alternative routes.[63] They concluded that terrorists now have the ability to distinguish transportation modes, and to manipulate crowdsourcing data on Waze or similar social navigation applications; terrorists could use this ability to orchestrate a gridlocked highway, facilitating an attack on the transportation system or affected areas.

In 2015, Gang Wang et al. further explored the potential malign use of Waze.[64] They observed that Waze uses weighted average algorithms to determine the most efficient path for navigation. Exploiting this through programming, the researchers then artificially introduced "slower" vehicle speeds, causing a traffic jam.[65] To prolong the congestion, they simply introduced additional "slower" vehicles into the area. The researchers also found that they could "hide" actual traffic congestion by programming "faster"-moving vehicles, thus falsely depicting free-flow traffic, which could entice users to take an obstructed route.[66] Malicious actors could potentially use this technique

[63] Meital Ben Sinai et al., *Exploiting Social Navigation* (Haifa, Israel: The Technion, 2014).

[64] Gang Wang et al., "Defending against Sybil Devices in Crowdsourced Mapping Services," paper presented at MobiSys '16, Singapore, June 25–30, 2016.

[65] Wang et al., "Defending against Sybil Devices," 4.

[66] Ibid., 5.

to either draw a large number of motorists into a dense area or to create traffic congestion in order to carry out a violent act on a large, condensed group.

Wang et al. also discussed a "man-in-the-middle" tactic that could effectively intercept communications between a mobile phone and Waze servers.[67] This technique essentially allows a malicious actor to replicate a Waze user's account in order to replicate thousands more accounts, and to potentially gain access to Waze servers, allowing the malicious actor to severely disrupt traffic behavior. Furthermore, they discovered that a Waze user's GPS location can be queried by identifying an individual and refreshing the app to locate and track their movements.[68] An individual can be tracked with enhanced accuracy through multiple falsely generated Waze accounts.[69] This technique, rather than affecting a large group of motorists, allows malicious actors to remotely stalk potential victims in a more target-specific manner.

C. SYNERGIES

Manipulating Waze demonstrates how SMSN can negatively impact transportation security. The Waze user community presents an excellent opportunity for SNA and social media analysis. There are no leaders among Waze users, but users are assigned value ratings when a traffic incident is reported—an individual's value rating increases when another Waze user confirms the reported incident, thus increasing the reporting user's credibility.[70] A high-credibility user might wield greater influence on the Waze community's larger driving behaviors, thereby affecting navigation patterns. A qualitative approach to analyzing social media exploitation and social navigation can be a first step in identifying potential related vulnerabilities to transportation security.

---

[67] Ibid., 4.

[68] Ibid., 5.

[69] Ibid.

[70] Chris Matysczyk, "Cops Accused of Fiddling with Their Locations on Waze to Fool Drivers," *CNET*, February 12, 2015, http://cnet.com/news/miami-cops-use-tech-to-fool-drivers-into-believing-theyre-not-there/.

D. CLOSING THE GAP

A gap still exists in current literature regarding specific impacts of SMSN on transportation security, particularly related to surface transportation systems. The study of surface transportation security within the context of a larger transportation infrastructure may contribute to a greater understanding of vulnerabilities and counter-measures associated with SMSN exploitation. In this context, the greater threat posed to public safety by the malign exploitation of SMSN vulnerabilities should also be explored.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

The research question—"What threats do SMSN pose to the surface transportation system?"—frames and guides the scope of this research. This thesis employs a qualitative analysis of surface transportation's vulnerabilities to malign use of SMSN applications in order to examine this question.

A. RELATIONSHIPS

The research first seeks to discover the relationship social networking, social media, and social navigation have with the surface transportation system. *Merriam-Webster* defines "relationship" as "the way in which two or more people, groups, countries, etc., talk to, behave toward, and deal with each other."[71] For the purposes of this thesis, we seek to establish how SMSN and transportation "behave toward, and deal with each other," which can be derived from available data. For example, the Transportation Research Board studied the uses of social media in public transportation.[72] The Board's findings synthesized the successful uses of social media to reach transit customers, explored how interaction with social media affected customers' transportation mode choices, and identified gaps and vulnerabilities in social media transportation apps. Similar research can help define the interaction of SMSN and transportation behavior, or vice-versa, and thus establish the relationship between SMSN and the surface transportation system.

This thesis hypothesizes that SMSN influence transportation behavior, and therefore create potential exploitable vulnerabilities in the transportation system. Confirming the relationship between transportation and SMSN may reveal commuters' growing dependence on these platforms and the implicit trust given to its users, who contribute and disseminate the information. The dependence and trust developed between

---

[71] *Merriam-Webster*, s.v. "Relationship," accessed November 4, 2015, http://www.merriam-webster.com/dictionary/relationship.

[72] Transit Cooperative Research Program, *Use of Social Media in Public Transportation—A Synthesis of Transit Practice* (Washington, DC: Transportation Research Board, 2012), http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_syn_99.pdf.

the application providers, users, and contributors increases the impact a malign actor can have by exploiting the transportation system's vulnerabilities.

B. VULNERABILITY CRITERIA

Having established the relationship between social media applications, social networks, and the surface transportation system, the vulnerability criteria must next be defined. In the context of this thesis, vulnerabilities are defined as the weak points in surface transportation security exposed—either intentionally or unintentionally—by SMSN. Exposure methods could include hacking, manipulating data, creating false information, crowdsourcing and disseminating false information, and using SMSN to gather intelligence for an attack. The transportation system is defined as components, in whole or in part, that contribute to the movement and navigation of people. These components consist of:

- transportation infrastructure such as bridges, highways, streets, control systems, and intelligent transportation systems[73]
- social media sites such as Facebook, Twitter, and Nextdoor
- social navigation sites such as Waze, Twittraffic, and Beat the Traffic
- mapping applications such as OpenStreetMap, MapQuest, and Google Maps

The Black Lives Matter protest on I-93 in Boston on January 15, 2015, exemplified the use of social media to organize a protest, but also exploited a vulnerability in Boston's transportation system. Using Facebook and Twitter, protestors organized a human barricade across I-93 that stopped traffic on one of the busiest highways in the Boston area.[74] Commuters were at a halt for four and a half hours.[75] Construction on I-93 and the Tip O'Neill Tunnel through Boston effectively removed surface streets. When the tunnel is congested, there are no other alternatives for motorists.

[73] Intelligent Transportation Systems are a collection of communication and traffic technologies that collect, disseminate and analyze information to improve efficiency, safety and smarter use of transportation.

[74] Peter Schworn, Laura Crimaldi, and John R. Ellement, "Protestors Snarl Morning Commute on I-92 near Boston," *Boston Globe*, January 15, 2015, https://www.bostonglobe.com.

[75] Ibid.

The protests virtually turned I-93 into a parking lot. Hypothetically, if a malicious actor had followed these events, they would have quickly realized the opportunity for an attack. This is one example of exposing weak points in the surface transportation system that could create a security risk. This thesis aims to uncover similar vulnerabilities and threats in the transportation system.

C. CATEGORIZATION

After the vulnerability criteria are defined, the next step is to categorize the threats. In doing so, this thesis includes the following:

- An examination of existing and known vulnerabilities that malign use of SMSN impose on the transportation system. This examination identifies how SMSN was used in past successful attacks, hacks, and disruptions to transportation systems. It also identifies thwarted attacks, hacks, and disruptions.

- An exploration of malign use of SMSN tools and tactics that have not yet been attempted. These potential threats are largely based on SMSN vulnerabilities uncovered in the research that could potentially disrupt surface transportation systems.

- Identification of standard hacks of websites, mobile applications, and mobile communications to determine vulnerable SMSN platforms. Documenting these attacks may show that hackers' basic tools and techniques are transferrable to SMSN platforms, enabling them to further exploit vulnerabilities in the surface transportation system.

- An investigation of general SMSN vulnerabilities to public safety, exploring hypothetical scenarios involving surface transportation security.

This research does not include a traditional vulnerability analysis. Before this type of analysis can be conducted, research must first explore, define, and understand the vulnerabilities. As a first step, a qualitative vulnerability analysis can provide insight into understanding how SMSN users purposely or mistakenly create vulnerabilities in the surface transportation system. A traditional vulnerability analysis, in which the vulnerabilities are rated in relation to severity and creation of security measures, could potentially be performed in later research once SMSN vulnerabilities to the surface transportation system have been identified.

Emerging trends in SMSN that could represent potential future vulnerabilities in the surface transportation system are beyond the scope of this research.

D. ANALYSIS

The threat categorization aims to provide a basic list and understanding of SMSN vulnerabilities. The categorization may also uncover trends relating to techniques, typical weak points, similarities between SMSN platforms with social media sites, and public use that make these systems vulnerable to malign exploitation. Lastly, the analysis makes projections about malicious or terrorist acts that could result from SMSN vulnerabilities. This discovery can enhance awareness of the potential devastation SMSN vulnerabilities and threats pose to the surface transportation system.

E. SOURCES

Primarily, this research reviews academic papers and journal articles, news articles, books, white papers, and websites. Additional data is gathered from technology-based conferences such as those held by BlackHat and Infiltrate.

Open-source information from popular social media and social navigation sites such as Twitter, Nextdoor, Waze, Inrix, and Twittraffic provide information that can be analyzed to determine how bad actors could exploit vulnerabilities in the transportation system. Investigating message boards and fora can also provide valuable information regarding vulnerabilities and user intent. Available metadata from these apps/websites may yield additional information regarding SMSN vulnerability and use.

F. OUTCOME

This research results in a catalog of malign SMSN tools, tactics, and techniques that pose security risks to surface transportation. It is hoped that this analysis may lead to a heuristic inquiry that could expose malign activities before they present a threat to the surface transportation system. This thesis provides homeland security professionals, cyber-security managers, city planners, and engineers a foundation upon which to anticipate and neutralize SMSN vulnerabilities to the transportation system.

IV. FINDINGS

This chapter discusses key relationships among the data that provide context for the research findings. First, the relationship between SMSN and surface transportation is established. Next, the chapter briefly describes how Web 2.0 platforms such as Waze, Google Maps, and Twitter work. Finally, a description of how terrorists use social media today is provided.

A. SMSN'S RELATIONSHIP WITH TRANSPORTATION

The evolution of the World Wide Web has enabled great innovation and collaboration among internet users. The rise of social media is considered Web 2.0's most defining characteristic.[76] Generally, social media is defined as "the collective of online communications channels dedicated to community-based input, interaction, content sharing and collaboration."[77] Popular social media sites such as Facebook, Twitter, and Google+ are examples of these online communications platforms. Many social media sites are designed for specific purposes or specific audiences. For example, LinkedIn is designed to engage and build a social network centered on business professionals; LinkedIn facilitates professional networking, allowing users to list work history and professional accomplishments, and to make employment connections.[78] At its heart, Web 2.0 allows users to exchange information within virtual and physical social networks. Web 2.0's strength is bringing people together, whether they are sharing playlists on Spotify (an online music-streaming service) or answering questions on Quora (a question-answer site, regulated by users).

Surface transportation has also been affected by the World Wide Web and social networking. For example, Facebook contains several social networking groups focused on driving safety. To understand these groups' influence on Facebook, researchers Emma

---

[76] *WhatIs*, s.v. "Web 2.0," accessed June 16, 2016, http://whatis.techtarget.com/definition/Web-20-or-Web-2.

[77] *WhatIs*, s.v. "Social Media," *WhatIs*, accessed June 16, 2016, http://whatis.techtarget.com/definition/social-media.

[78] *Wikipedia*, s.v. "Linkdedin," accessed June 16, 2016, https://en.wikipedia.org/wiki/LinkedIn.

Apatu, Melissa Alperin, Kathleen Miner, and David Wiljer sought to measure its effectiveness. Their research discovered that social networking has been an effective tool in promoting safe driver behavior. "In all," they found, "62% of respondents <24 years and 57.8% of respondents aged >25 years reported changing their driving-related behaviors as a result of reading information on the [driving safety Facebook groups] to which they belong."[79] Some researchers argue that this type of descriptive data (or sentiment) is more useful to motorists than traditional data collection techniques such as inductive loops or video detection.[80] While traditional data simply relays facts and numbers, sentiment often conveys an emotional state or a perception about a situation, person, or group, which helps traffic engineers better understand the human effects of driving.[81]

Twitter, the micro-blogging social media site, has become a sounding board for users to express their frustration with others' driving behavior, or a means to warn others about traffic conditions.[82] The use of Twitter to express traffic and transportation sentiment has become so prevalent that researchers have begun to correlate tweets with mobility patterns in an effort to understand a particular area's overall traffic background.[83] In some cases, Twitter users have become social sensors for traffic conditions; programs designed to provide directions based on geolocation can now alter directions based on Twitter input.[84]

---

[79] Emma Apatu et al., "A Drive through Web 2.0—An Exploration of Driving Safety Promotion on Facebook," *Health Promotion Practice* 14, no. 1 (January 2013): 93.

[80] Panraphee Raphiphan, Arkady Zaslasky, and Maria Indrawan-Santiago, "Building Knowledge from Social Networks on What Is Important to Drivers in Constrained Road Infrastructure," paper presented at the 18th International Conference on Knowledge Based and Intelligent Information & Engineering Systems, Gydnia, Poland, 2014, 728.

[81] Stefan Stieglitz and Linh Dang-Xuan, "Emotions and Information Diffusion in Social-Media—Sentiment of Microblogs and Sharing Behavior," *Journal of Management Information Systems* 29, no. 4, (April 2013): 218.

[82] Theodore Georgiou et al., *Mining Complaints for Traffic Jam Estimation: A Social Sensor Application* (Santa Barbara: University of California Santa Barbara, 2015): 1.

[83] Francisco Rebelo, Carlos Soares, and Rosaldo Resetti, "TwitterJam: Identification of Mobility Patterns in Urban Centers based on Tweets," paper presented at the 2015 IEEE First International Smart Cities Conference (ISC2), Guadalajara, Mexico, October 25–28.

[84] Silvio Ribeiro et al., "Traffic Observatory: A System to Detect and Locate Traffic Events and Conditions Using Twitter," paper presented at the 5th ACM Sigspatial International Workshop on Location Based Networks, Redondo Beach, CA, November 6, 2012.

Transportation agencies have noticed the power of social media and have started using various social media platforms to reach motorists. Table 1 shows an example of some California transportation agencies that use social media.

Table 1. Social Media Use by California Transportation Agencies

Agency	Social Media Platforms
California Department of Transportation (CalTrans)	Twitter, Facebook, YouTube, Google+, Waze
City of Los Angeles Department of Transportation (LADot)	Twitter, Facebook, YouTube, Instagram,
San Francisco Municipal Transportation Agency (SFMTA)	Twitter, Facebook, YouTube
City of San Jose Department of Transportation	Twitter, Facebook

Social media is a valuable tool for these agencies because it helps them "understand the needs, behaviors and preferences of people to improve and support transportation-related decisions during emergency and non-emergency situations."[85] Social media can also help transportation agencies distribute information regarding upcoming transportation-related construction work or sudden traffic delays in an effort to reduce traffic congestion.

In April 2016, the California Department of Transportation (CalTrans) announced a partnership with Waze that will allow both parties to exchange real-time traffic information. Waze will provide CalTrans with real-time traffic data from its users (anonymous data), which will be posted on CalTrans' traffic maps. In turn, CalTrans will provide Waze with road construction work notices and other traffic information that could contribute to congestion.[86] This effort aims to empower motorists with the information needed to make effective driving decisions when traveling or commuting

[85] Aybek Kocetepe et al., "The Reach and Influence of DOT Twitter Accounts: A Case Study in Florida," paper presented at the 18th International Conference on Intelligent Transportation Systems, Canary Islands, Spain, September 15–18, 2015.

[86] "Caltrans Partners with Waze Connected Citizens Program," California Department of Transportation, April 5, 2016, http://www.dot.ca.gov/paffairs/pr/2016/prs/16pr033.html.

throughout California. This partnership exemplifies the expanding relationship between transportation and social media and the power of information sharing.

B. GOOGLE MAPS, WAZE, AND TWITTER

This section provides a brief description of Google Maps, Waze, and Twitter as they are used for transportation information. A basic understanding of these platforms also provides insight into how they can be used for malicious purposes.

1. Google Maps and Google Earth

Google Maps, first launched in 2005, offers "satellite imagery street maps, 360° panoramic views of streets, real-time traffic conditions and route planning for traveling by foot, car, bicycle or public transportation."[87] Figure 1 shows the typical directions function on the Google Maps website.

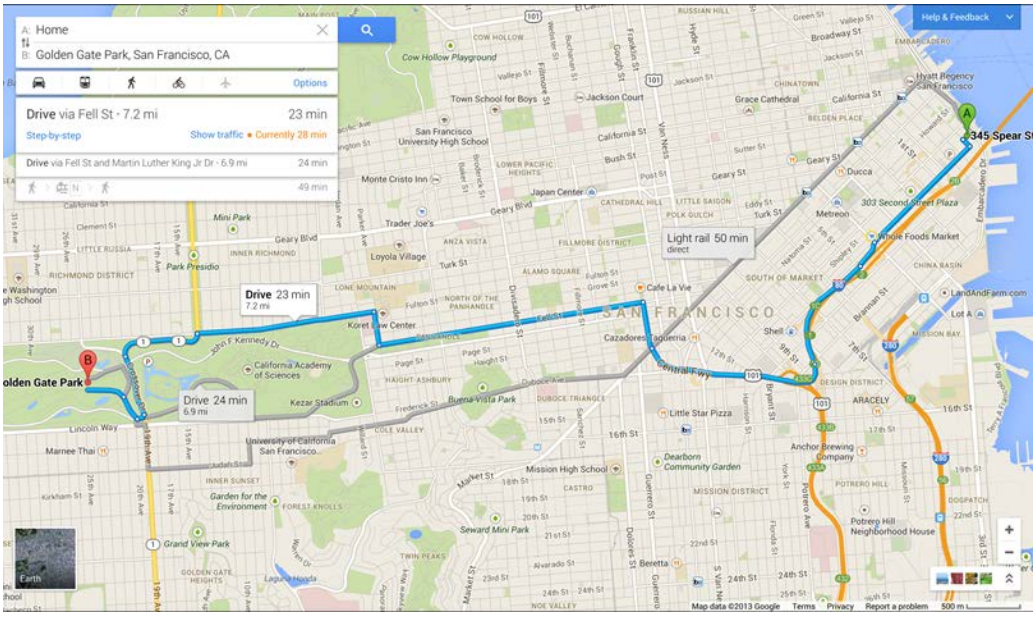


Figure 1. Google Maps[88]

[87] *Wikipedia*, s.v. "Google Maps," accessed June 14, 2016, https://en.wikipedia.org/wiki/Google_Maps.

[88] Drew Olanoff, "Deep Dive with the New Google Maps for Desktop with Google Earth Integration, It's More than Just a Utility," Tech Crunch, May 15, 2013, https://techcrunch.com/2013/05/15/deep-dive-with-the-new-google-maps-for-desktop-with-google-earth-integration-its-more-than-just-a-utility/.

In 2008, Google developed Google Maps for the mobile device, which provides motorists turn-by-turn driving directions.[89] To obtain real-time traffic information for the app, Google uses signals from cellphones to create a traffic conditions map.[90] A cellphone registers its location each time it passes by a cellphone receiving tower; the Google Maps algorithm is able to use this data to determine a traveling vehicle's speed. It can also compare data from other cellphone signals, which ultimately creates the background conditions for a traffic congestion map. Google further leverages its millions of users through a program called MapMaker to develop additional mapping information—this program is used in areas where accurate mapping data is not available and local knowledge is needed.[91]

Google Maps is accessible via the internet; another Google product with similar mapping and geographic capabilities, Google Earth, is only accessible as a standalone application that must be downloaded to a computer or mobile device.[92] Google Earth combines satellite imagery, aerial photography, and geographical information systems and superimposes this information on a three-dimensional earth.[93] One advantage of Google Earth over Google Maps is the "street view" feature. Street view "provides 360° panoramic street-level views and allows users to view parts of selected cities and their surrounding metropolitan areas at ground level."[94] This feature visually familiarizes the user exploring new destinations and areas. Other key features of Google Earth that provide advantages over Google Maps are the "birds-eye view" and "3D" capabilities.[95] These features provide additional points of view and data sets for the user to exploit.

---

89 Ibid.

90 Greg Miller, "The Huge, Unseen Operation behind the Accuracy and Operation of Google Maps," *Wired*, December 8, 2014, http://www.wired.com/2014/12/google-maps-ground-truth/.

91 Ibid.

92 *Wikipedia*, s.v. "Google Earth," *Wikipedia*, accessed August 7, 2016, https://en.wikipedia.org/wiki/Google_Earth

93 Ibid.

94 Ibid.

95 Ibid.

2. Waze

Purchased by Google in 2013, Waze is a traffic and geographical navigation application that provides turn-by-turn navigation, travel times, and route details to its users (see Figure 2).[96] When the app is activated, Waze passively collects and processes GPS information from user cell phone transmissions to yield speed, direction, and location information.[97] Waze had an estimated 50 million users at the time of Google's purchase.[98]

Figure 2. Waze[99]

---

[96] *Wikipedia*, s.v."Waze," accessed June 14, 2016, https://en.wikipedia.org/wiki/Waze.

[97] Talia Dror, Sagi Dalyot, and Yerach Doysther, "A Quantitative Geo-Evaluation of Crowdsourcing and Wisdom of the Crowd," International Federation of Surveyors, December 2014, 6, http://www.fig.net/resources/monthly_articles/2014/december_2014/december_2014.pdf.

[98] Josef Federman and Max J. Rosenthal, "Waze Sale Signals New Growth for Israeli High Tech," Yahoo, June 12, 2013, https://www.yahoo.com/news/waze-sale-signals-growth-israeli-high-tech-174533585.html?ref=gs.

[99] Perez, "Navigation App Waze."

What differentiates Waze from other traffic navigation applications, however, is the additional focus on gathering and disseminating traffic information from its users. Waze users, or "Wazers," are able to contribute and post traffic information such as destinations, traffic congestion, accidents, road closures, and available routes based on real-time observations. This "wisdom of the crowd" is used to help solve daily commuting and vehicle travel issues. As users drive and post traffic information, they accrue credibility points. As points accumulate, users are assigned ranks ranging from "Waze Baby" to "Waze Royalty."[100] "Waze Champs" are higher-level Waze users and editors with seniority who are active in fora and the Waze wiki.[101] Waze Champs ultimately approve editing of maps and help Waze ensure information is as accurate as possible. The point system and user level recognition function as incentives for Wazers to keep using the app, and as a way to provide information checks and balances, allowing users to trust the information.

3. Twitter

Twitter is a micro-blogging SMSN platform. Each micro-blog post consists of 140 characters, which are called tweets.[102] A Twitter user establishes their network by "following" other users. All users on Twitter can view all tweets, unless access is restricted to those within one's network. Twitter users typically "share their thoughts, news, and information."[103] Messages on Twitter can also be "re-tweeted" (re-posted) by other users to spread the message among the network.[104] To denote key words or topics, a hashtag (#) is placed before the word or topic.[105] The hashtag helps categorize content

---

[100] "Your Rank and Points," Wiki Waze, accessed June 14, 2016, https://wiki.waze.com/wiki/Your_Rank_and_Points#Waze_Points_Level_.28in_client_app.29.

[101] Ibid.

[102] *Wikipedia*, s.v. "Twitter," accessed June 14, 2016, https://en.wikipedia.org/wiki/Twitter.

[103] Brandon Smith, "The Beginner's Guide to Twitter," *Mashable*, June 5, 2012, http://mashable.com/2012/06/05/twitter-for-beginners/#QsuAfs2B5Eq7.

[104] Chris Syme, "Why Do You Retweet?" *Social Media Today*, July 23, 2010, http://www.socialmediatoday.com/content/why-do-you-retweet.

[105] Rebecca Hiscott, "The Beginner's Guide to Hashtag," *Mashable*, October 8, 2013, http://mashable.com/2013/10/08/what-is-hashtag/#FgiK4gv7euqL.

and ensure that it is searchable.[106] Twitter can be accessed through the internet, as well as through mobile applications for tablets and smartphones. Twitter's basic technological framework relies on available open-source software for web-application interface setup, message handling, and delivery.[107] Twitter also allows geotagging (geographically locating a tweet).[108] As of March 2016, Twitter had over an estimated 310 million active users.[109]

One of Twitter's most common uses is to crowdsource information and opinions. For example, during and after Hurricane Sandy, Twitter was widely used by "individuals, first responder agencies and utility companies to relay messages and information, share evacuation orders and provide updates on the storm."[110] The Federal Emergency Management Agency (FEMA) used Twitter during Hurricane Sandy for situational awareness, utilizing trending topics to produce safety information.[111] Government agencies at the state level also use Twitter to inform their networks about road conditions and construction (see Figure 3).

[106] Ibid.

[107] Ibid.

[108] Ibid.

[109] *Wikipedia*, s.v. "Twitter," accessed June 14, 2016, https://en.wikipedia.org/wiki/Twitter.

[110] Sean Estes Cohen, "Sandy Marked a Shift for Social Media Use in Disasters," *Emergency Management*, March 7, 2013, http://www.emergencymgmt.com/disaster/Sandy-Social-Media-Use-in-Disasters.html.

[111] Ibid.

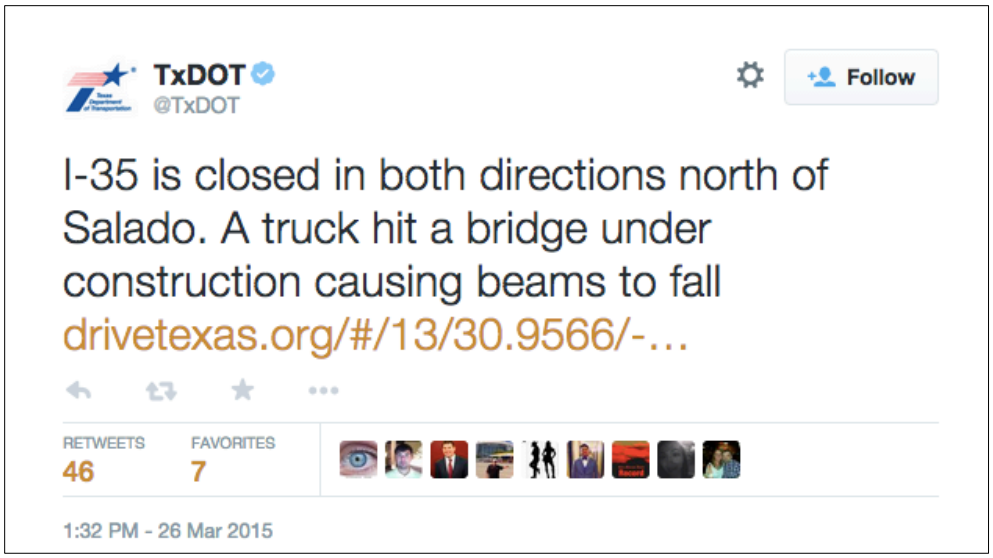


Figure 3. Tweet from the Texas Department of Transportation[112]

Waze has also partnered with Twitter to distribute traffic-related information through the Twitter platform. In terms of traffic and transportation, numerous studies have been performed to analyze traffic sentiment and traffic conditions based on tweets.[113]

Platforms such as Google Maps, Waze, and Twitter leverage their many users to crowdsource traffic- and transportation-related information in order to enhance and improve traffic operations. Unfortunately, despite their benefits, no social media platform is immune to malicious acts or activity.

C. TERRORIST USE OF SOCIAL MEDIA

A simple Google search of "terrorist use of social media" yields 19,200,000 results. While not every result is a unique example of social media exploitation by terrorists, the sheer number of results illustrates the amount of analysis and discussion on this topic.

---

[112] "1 Dead, Several Injured after Major Bridge Accident; Traffic Rerouted all along I-35 North of Austin," Texas Public Radio, March 26, 2015, http://tpr.org/post/1-dead-several-injured-after-major-bridge-accident-traffic-rerouted-all-along-i-35-north-austin#stream/0.

[113] For example, see Antonio Candelieri and Francesco Archeti, "Detecting Events and Sentiment on Twitter for Improving Urban Mobility," paper presented at ESSEM 2015, Istanbul, May 5, 2015.

Social media is easy to use, inexpensive, and widely accessible. These characteristics make it attractive to both the mainstream public and malicious actors. Social media can be a tool that helps terrorists further their goals, whatever they may be. The three most common uses of social media by terrorists and radicalized movements include communication, development and distribution of terrorist propaganda, and the recruitment of new members.[114] ISIS, for example, has developed sophisticated social media skills, proving "fluent in YouTube, Twitter, Instagram, Tumblr, internet memes and other social media."[115] ISIS is successful because they use social media to bring their malicious message to the world's front door.[116] Savvy social media use "increases the number of people learning about your cause, [spreads] the word, and supports your organization," which is exactly how ISIS conducts their social media activities.[117] ISIS has exploited these social media platforms by displaying video beheadings, posting messages for a call to arms to wage *jihad* in the West, and conducting secret communications on encrypted messaging services, which conveys the communication, propaganda, and recruitment objectives they pursue (see Figure 4).[118]

---

[114] "The Role of Technology in Modern Terrorism," INFOSEC Institute, February 3, 2016, http://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/.

[115] "How Terrorists Are Using Social Media," *Telegraph*, November 4, 2014, http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html.

[116] Wu, "Impossible to Regulate," 289.

[117] "Social Media on Purpose 2014—Using Social Media Strategically to Advance Your Mission," *Stanford Social Innovation Review*, accessed May 22, 2014, http://ssir.org/socialmediaonpurpose.

[118] Brenden K. Koerner, "Why ISIS Is Winning the Social Media War," *Wired*, April 2016, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/.

Figure 4. Example of ISIS' Social Media Use[119]

ISIS and other terrorist groups can also use social media for fundraising and intelligence gathering, and to conduct cyberattacks and distribute training materials.[120] The continued exposure and exploitation of vulnerabilities in social media—and now social navigation—is a major concern for homeland security professionals, including those charged with securing the surface transportation system.

D. TYPES OF THREATS/ATTACKS BASED ON VULNERABILITY

Data on SMSN vulnerabilities in the surface transportation system were derived from a review of existing academic papers, journal articles, news articles, books, white papers, and websites. Table 2 lists vulnerabilities already discovered by researchers or already exploited by terrorists. The vulnerabilities are grouped into three categories: SMSN manipulation, social navigation manipulation, and use of SMSN for intelligence.

[119] Chris Good, Joshua Cohan, and Lee Ferran, " 'Cybervandalism': ISIS Supporters Hijack U.S. Military Social Media Accounts," ABC News, January 12, 2015, http://abcnews.go.com/International/us-military-twitter-account-apparently-hijacked-isis-supporters/story?id=28170963.

[120] "The Role of Technology in Modern Terrorism," INFOSEC Institute.

Table 2. Existing and Known Vulnerabilities

Group/ Individual	*Scenario*	*SMSN Manipulation (Facebook, Twitter)*	*Social Navigation Manipulation (Waze, Google)*	*Use of SMSN for Intelligence*
Researchers	Generated false information/events on Waze		x	
Researchers	Attack on real-time trip routing function on Waze		x	
Researchers	Large-scale attack via virtual vehicles or “ghost riders” on Waze		x	
Researchers	Generation of false information or events on Google Maps		x	
Terrorists	Use of Google Earth/Maps for intelligence			x
Terrorists	Use of Google Earth for intelligence			x
Hackers	Hacking/spamming of Google Maps with false information		x	
Researchers	Generation of false information/events on Waze		x	
Researchers	Attack on real-time trip routing function on Waze		x	
Researchers	GPS spoofing on Waze		x	
Researchers	Use of man-in-the-middle and Sybil attack to influence traffic routing on Waze		x	

One definition of manipulation is "the action of influencing or controlling something to your advantage, often without anyone knowing it."[129] Social media are freely available, and their users generate content ranging from pictures and videos, to web posts and text.[130] Manipulating social media or social navigation platforms thus involves using or influencing that content to one's advantage. In the same vein, intelligence can be defined as "the ability to acquire and apply knowledge and skills."[131] For the purposes of this thesis, intelligence is the information acquired and disseminated on SMSN platforms for the application of malign intent, to include the identification of potential attack targets and use in the planning and execution process.

Table 3 lists potential vulnerabilities based on past manipulation and/or intelligence-gathering use of social media. The last two entries in Table 3 reflect vulnerabilities in the rapidly evolving autonomous-vehicle market. The vulnerabilities are illustrated by scenarios and grouped into four categories: SMSN manipulation, social navigation manipulation, use of open-source SMSN for intelligence, and social media to control narrative and information.

---

[129] *Cambridge Dictionary*, s.v. "Manipulation," accessed July 5, 2016, http://dictionary.cambridge.org/us/dictionary/english/manipulation.

[130] Freeman and Schroeder, *Social Media Exploitation*, 10.

[131] *Oxford Dictionaries*, s.v. "Intelligence," accessed July 13, 2016, http://www.oxforddictionaries.com/us/definition/american_english/intelligence.

Table 3. Potential Vulnerabilities

Group/ Individual	*Scenario*	*SMSN Manipulation (Facebook, Twitter)*	*Social Navigation Manipulation (Waze, Google)*	*Open Source SMSN Information as Intelligence*	*Social Media to Control Narrative and Information*
Researchers	Use of geosocial networks to improve traffic safety—conversely, potential use by terrorists for intelligence			x	
Researchers	Use of social media platforms such as Waze to improve driving conditions		x	x	
Researchers	Use of social media platforms such as Twitter to distribute and review information			x	x
Terrorists	Hacking of state and local social media accounts	x	x		x
Researchers	Use of cloning attack to generate false events or attack real-time routing function		x		
Researchers	Use of Sybil attacks in Vehicle Area Networks (VANETS) and on-board social networks		x		
Researchers	Use of cyberattacks on connected vehicles and on-board social networks		x		

The information in Tables 2 and 3 fit within the framework of the vulnerability criteria described in Chapter III. Chapter V provides a more detailed illustration of how malicious actors could exploit these vulnerabilities to put the surface transportation system at risk.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS

Prior to evaluating the data from Chapter IV, it is necessary to better understand the potential value SMSN tools represent for terrorists.

A. THE VALUE OF SMSN TOOLS FOR TERRORISTS

"Terrorists use social media for many of the same reasons that anyone else does. It is user friendly, reliable and free."[132] Social media can easily provide information to terrorists who are planning an attack, whether it be intelligence on specific targets, optimal times of day for an attack, or an estimated number of potential casualties. Similarly, social navigation and mapping technology can provide terrorists with information about potential targets, ingress/egress routes, and potential infrastructure damage and disruption.

The 2008 attacks in Mumbai by the jihadist group Lashkar-e-Taiba exemplify how terrorists can leverage social media to conduct their operations. During the attacks, Lashkar-e-Taiba monitored Twitter to enhance their situational awareness; they were able to evaluate how their attack was unfolding in the eyes of their victims, and identify potential law enforcement operations.[133] This information allowed the group to evade authorities and continue their terror operations. Lashkar-e-Taiba also leveraged social navigation and mapping technology (such as Google Maps and Google Earth) to identify attack targets and route planning.[134]

Malicious actors can also monitor social media to ensure their attacks coincide with known and planned gatherings, increasing potential lethality. For example, during the Ferguson, Missouri Protests in 2015, "Twitter, Facebook and Tumblr [were used] to

[132] Wu, "Impossible to Regulate," 288.

[133] Oh, "Information control and terrorism," 33

[134] Matteo Cavalini and John Austen, *Terrorist Use of the internet* (Egham, UK: Royal Holloway, 2014), 3.

spread the word about planned protest locations."[135] In a hypothetical scenario, malicious actors could have monitored Twitter, Facebook, and Tumblr to identify protest locations as potential attack targets. Further, Google Maps could be used to exploit vulnerabilities in the transportation system to enhance an attack.

On a macroscopic level, SMSN gives malicious actors access to a captive audience with a "follow-the-crowd" mentality.[136] Malicious actors may influence this audience by injecting misleading information or manipulating data to control their behavior for an eventual attack on the transportation system. This, however, requires skills in manipulating social media. The following section describes the sophistication malicious actors need in order to exploit SMSN.

B. ANALYSIS

To reiterate, the research question posed in this thesis is, "What threats do SMSN pose to the surface transportation system?" As described in the literature review, research is needed (and is ongoing) to specifically identify the threats and vulnerabilities SMSN pose for surface transportation systems.

1. Social Media

There is no conclusive evidence suggesting that social media pose a direct threat to surface transportation systems. However, social media's potential for exploitation is implied by its pervasive use among terrorist groups and individuals. The most concerning exploitation of social media comes in two forms: disseminating false information to control the narrative or behavior of social groups, and using legitimate information as a source of intelligence.

---

[135] Rubina Madan Fillion, "How Ferguson Protestors Used Social Media to Organize," *Wall Street Journal*, November 24, 2015, http://blogs.wsj.com/dispatch/2014/11/24/how-ferguson-protesters-use-social-media-to-organize/.

[136] Amble, "Combating Terrorism," 340–341.

a. Disseminating False Information

Many government transportation agencies maintain social media accounts on platforms such as Facebook, Twitter, and Nextdoor to disseminate traffic-related information. In doing so, they provide their followers information that informs traveling and commuting decisions. They are also able to directly suggest traveling and commuting actions. Terrorists have the ability to hack into social media accounts and have been known to do so to control the political and terror message.[137] In a hypothetical scenario, terrorists could hack into one or several transportation agencies' social media accounts to distribute false information and to influence traffic routing to set up an attack. Alternatively, terrorist or malicious actors, as "followers" of a transportation agency's social media account, can suggest traffic routing based on false traffic events. In either scenario, terror operations could be conducted using vehicle-born explosives or pre-staged explosives along congested traffic routes recommended through social media.

How feasible is this scenario? Although a detailed assessment of specific threats is out of the scope of this thesis, this research does seek to identify potential exploitable vulnerabilities. That being said, homeland security professionals and emergency responders are constantly evaluating social media information for legitimacy prior to acting on such information. Social media has been an asset for disaster response, but it has been a challenge for homeland security professionals to discern creditable, actionable information.[138] While not associated with SMSN transportation systems, the social media postings of the San Bernardino Terrorists (Syed Farook and Tashfeen Malik) and the Orlando Terrorist (Omar Mateen) relating to their ties to terrorist groups illustrate that social media information is difficult to substantiate, thus limiting the chances for a successful investigation leading to an arrest.[139]

---

[137] Seth Rosenblatt, "US Military Social Media Accounts Hacked," CNET, January 12, 2015, http://www.cnet.com/news/us-military-social-media-accounts-hit-with-hacking-attack/.

[138] Seth Thomas, "Social Media Changing the Way FEMA Responds to Disasters, *National Defense*, September 2013, http://www.nationaldefensemagazine.org/archive/2013/September/Pages/SocialMediaChangingtheWayFEMARespondstoDisasters.aspx; Lindsay, "Social Media and Disasters," 6.

[139] David Gomez, "How Did the FBI Miss Omar Mateen," *Chicago Tribune*, June 14, 2016, http://www.nationaldefensemagazine.org/archive/2013/September/Pages/SocialMediaChangingtheWayFEMARespondstoDisasters.aspx.

b. Using Legitimate Information as Intelligence

Social media platforms provide a forum for users to update explicit and implicit information to and about their social networks.[140] Twitter, for example, allows speedy and concise messages that can propagate beyond one's network through re-tweeting, ultimately becoming a source of traceable information.[141] During natural disasters, Twitter has been used to provide situational awareness of the affected area. Emergency responders can track Twitter trends and make decisions about rescue efforts.[142]

Twitter is also commonly used to express sentiment regarding traffic conditions. Researchers have developed an algorithm to extract traffic-related tweets as a tool to monitor traffic conditions, and have created software that visually maps these tweets to better understand the performance of the surface transportation system.[143] This analysis of traffic-related tweets is a form of intelligence gathering, which researchers hope will be used to improve the flow of vehicle traffic. Malicious actors can likewise exploit this information as tactical knowledge to attack the surface transportation system.

As previously mentioned, Lashkar-e-Taiba used Twitter to gather situational awareness during their 2008 attacks in Mumbai. A malicious group could similarly track traffic-related tweets to determine and target vulnerable locations within the surface transportation system. Public transportation has been a popular target for terrorists, and tweets regarding service disruptions or delays in transit could be evaluated for an

---

[140] Davide Frey, Arnaud J´egou, and Anne-Marie Kermarrec, "Social Market: Combining Explicit and Implicit Social Networks," paper presented at the International Symposium on Stabilization, Safety, and Security of Distributed Systems, Grenoble, France, October 2011, 1–2.

[141] Jayson DeMers, "Twitter vs. Facebook: How Do the They Compare?" *Huffington Post*, September 5, 2013,http://www.huffingtonpost.com/jayson-demers/twitter-vs-facebook_b_3869786.html.

[142] Alisa Kongthon et al., "The Role of Twitter during a Natural Disaster: A Case Study of the 2011 Thai Food," paper presented at PICMET '12: Technology Management for Emerging Technologies, Vancouver, British Columbia, July 29–August 2, 2012), 2231.

[143] Kaiquan Fu, Chang-tien Lu, Rakesh Nune, and Jason Tao, "Steds: Social Media based Transportation Event Detection with Text Summarization," paper presented at the 2015 IEEE 18th International Conference on Intelligent Transportation Systems, Canary Islands, Spain, September 15–18, 2015, 1952; Rebelo, Soares, and Resetti, "TwitterJam," 2–3.

attack.[144] Delays or service disruptions leave many riders stranded at public transit stations that are in turn vulnerable to an attack. For example, a simple search of the #BARTstrike hashtag (see Figures 5 and 6) could provide enough information for a malicious group to determine if an attack on the San Francisco Municipal Railway or Caltrain transportation systems is feasible and substantial. Open-source information is freely available on social media; with sufficient planning and intent, terrorists could use this information to plot an attack.

Figure 5. #BARTstrike Tweet with Time and Location Tags[145]

[144] Brian Michael Jenkins and Bruce R. Butterworth, *Troubling Trends in Terrorism and Attacks on Surface Transportation: The Outlook is Grim, but People Still Have a Great Deal of Control* (San Jose, CA: Mineta Transportation Institute, 2015), 2.

[145] "The BART Strike in Pictures and Tweets," *Wall Street Journal*, July 2, 2013, http://blogs.wsj.com/digits/2013/07/02/the-bart-strike-in-pictures-and-tweets/.

Figure 6. #BARTstrike Tweet with Population Information[146]

2. Social Navigation Manipulation

Ongoing research is investigating vulnerabilities in Waze and Google Maps that could leave the apps open to exploitation by terrorists or other malign actors.[147] Sybil attacks are a primary focus of this research. A Sybil attack is a type of hacking on Web 2.0 platforms in which a malicious actor creates multiple false identities to hijack and control a system or to influence a reputation system.[148] Figure 7 shows a simple graphical representation of a Sybil attack.

[146] Ibid.

[147] Gang Wang et al., "Defending against Sybil Devices in Crowdsourced Mapping Services," paper presented at MobiSys '16, Singapore, June 25–30, 2016; Ben Sinai et al., *Exploiting Social Navigation*; Tobias Jeske, "Floating Car Data from Smartphones—What Google and Waze Know about You and How Hackers Can Control Traffic," paper presented at Black Hat Europe, Amsterdam, March 12–15, 2013.

[148] Alexander Howard, "What is a Sybil Attack," TopTen Reviews, August 2, 2011, http://anti-virus-software-review.toptenreviews.com/what-is-a-sybil-attack-.html.

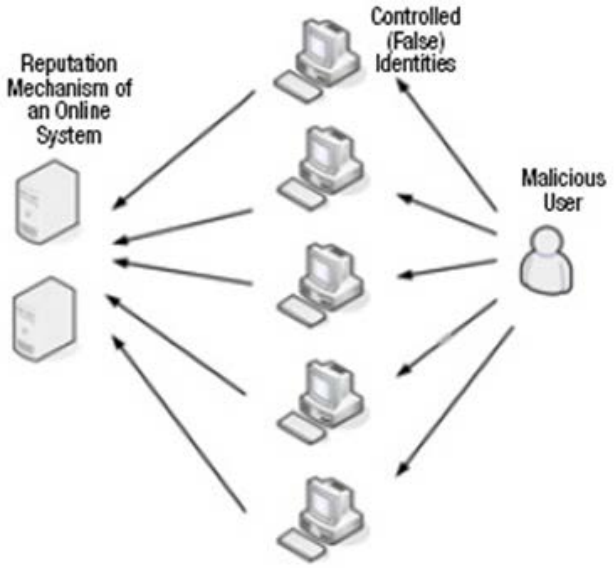


Figure 7. Sybil Attack[149]

Several groups of researchers have conducted Sybil attacks in two ways. First, one group implemented an operating system emulator on a computer and used script software to generate false user accounts in Waze.[150] A second method conducted a man-in-the-middle attacks, which was used to intercept wireless communications traffic between the mobile device and the application server. This was performed both on Waze and Google Maps (see Figures 8 and 9).[151] Either method of Sybil attack could arm a malicious actor with multiple imposter identities.[152]

---

[149] Ladislav Beranek, "JOnline: Auditing Electronic Auction Systems," ISACA, accessed August 14, 2016, http://www.isaca.org/Journal/archives/2010/Volume-4/Pages/JOnline-Auditing-Electronic-Auction-Systems.aspx.

[150] Wang et al., "Defending against Sybil Devices," 3; Ben Sinai et al., *Exploiting Social Navigation*, 5; Jeske, "Floating Car Data from Smartphones," 2.

[151] Wang et al., "Defending against Sybil Devices," 4; Jeske, "Floating Car Data from Smartphones," 2.

[152] It should be noted that Wang et al. received Institutional Review Board permission to conduct Sybil attack experiments in locations with low population densities and where low traffic volumes were expected; they were instructed to terminate the experiment should actual Waze users be affected. Sinai et al. conducted their experiment in Haifa, Israel; to ensure safety of actual Waze users, they avoided major roads and highways. Jeske conducted his experiment on roads in Hamburg-Bahrenfeld, Germany; it is not known how Jeske ensured motorist safety during his experiment. See Wang et al., "Defending against Sybil Devices," 2–3; Ben Sinai et al., *Exploiting Social Navigation*, 5; Jeske, "Floating Car Data from Smartphones," 8.

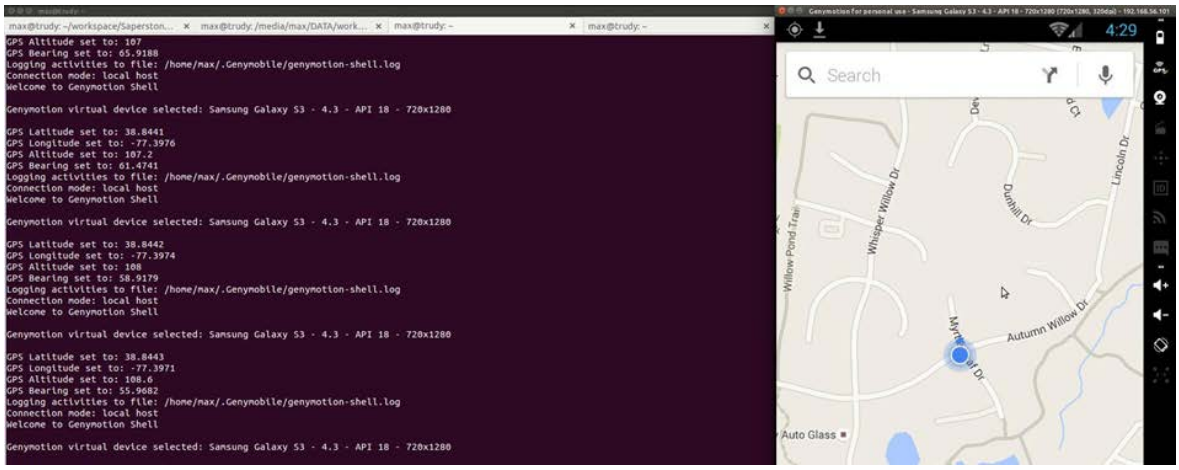


Figure 8. Example Software Script on an Operating System Emulator[153]

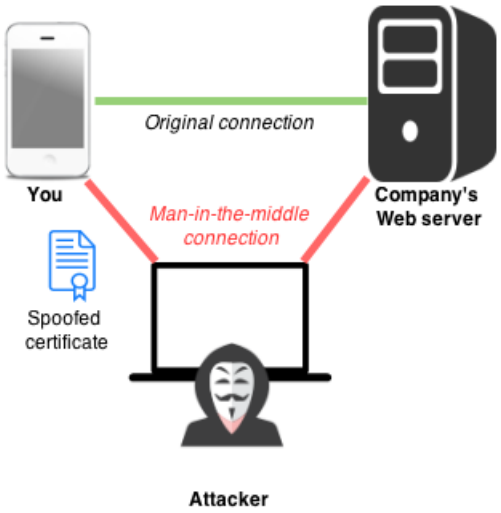


Figure 9. Main-in-the-Middle Attack[154]

Waze and Google Maps depend on crowdsourced information automatically drawn from mobile devices or directly input by users. Algorithms then use this information to determine surface transportation choices for the user based on starting and

[153] Max Saperstone, "Using Genymotion to Simulate a Moving Device," coveros, November 10, 2015, https://www.coveros.com/using-genymotion-to-simulate-a-moving-device/.

[154] "What Is Man-in-the-Middle and How to Protect Your Data and Mobile Apps from Such Attacks," TeskaLabs, accessed August 14, 2016, https://www.teskalabs.com/blog/protect-mobile-app-and-prevent-man-in-the-middle-attack.

destination locations. A Sybil attack exploits trust vulnerabilities in web and mobile application platforms by disregarding the terms of use agreements (which preclude the deliberate introduction of false information) and using imposter identities.[155] These imposter identities can present false or alternative information that incorrectly guide users in a manner desired by the malicious actor. Thousands of false identities can also be programmed to operate in a particular manner such that users are misled to "follow the crowd."

a. Waze

In Waze, imposter identities can affect surface traffic behavior in four ways:

1. An imposter identity can plant false traffic data points such as accidents, road closures, hazards, police locations, and traffic congestion.[156]
2. Numerous imposter identities can be programmed to drive slowly or quickly along a particular route and create traffic congestion, as long as the number of imposter vehicles outnumbers actual vehicles.[157]
3. A malicious actor can program thousands of imposter identities, or "ghost riders," to travel at various speeds to trigger traffic congestion and promote alternate routes on Waze.[158]
4. Imposter vehicles can use mock GPS coordinates to travel along a certain trajectory at programmed speed intervals, thus creating traffic congestion and promoting alternate routes.[159]

In the research cited, methods two through four caused Waze to display traffic congestion. Waze will suggest alternate travel routes should the targeted route have a comparably longer travel time.[160] Method one, in and of itself, does not affect traffic routing; it may, however, potentially influence an actual motorist to take alternate

---

[155] "Terms of Use," Waze; "Google Maps/Google Earth Additional Terms of Service," Google.

[156] Wang et al., "Defending against Sybil Devices," 3.

[157] Ibid., 4.

[158] Ibid., 5.

[159] Ben Sinai et al., *Exploiting Social Navigation*, 5.

[160] Wang et al., "Defending against Sybil Devices," 4.

routes.[161] Figures 10 through 12 display the various Sybil attacks and the Waze app's resulting reactions. Figure 10 shows placement of false police locations by the student researchers at Technion. There was no conclusive evidence that Waze would have displayed an alternate route; ultimately, Waze users themselves must make the determination to use alternate routes.

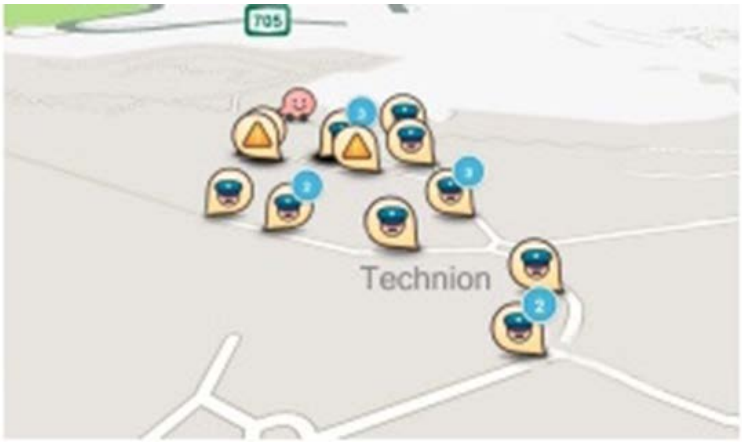
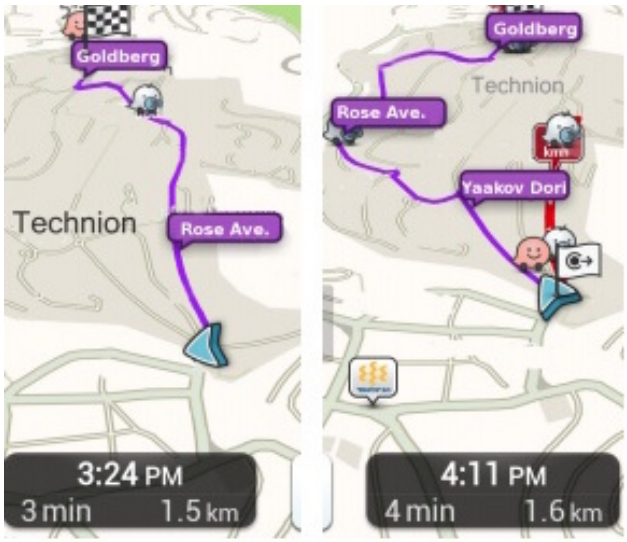


Figure 10. False Waze Locations[162]

Figure 11 shows the student researchers' false traffic congestion created by Sybil identities. Waze reacted by displaying an alternate route.

[161] Ben Sinai et al., *Exploiting Social Navigation*, 4.

[162] Ben Sinai et al., *Exploiting Social Navigation*.



(a) Pre-attack route (b) Post-attack route

Figure 11. False Traffic Congestion in Waze from Technion Students' Sybil Attack[163]

Figure 12 shows the false traffic congestion created by the Wang et al.'s Sybil identities. Waze reacted by displaying an alternate route.

Figure 12. False Traffic Congestion in Waze from Wang et al.'s Sybil Attack[164]

[163] Ibid.

[164] Wang et al., "Defending against Sybil Devices."

b. Google Maps

Much like in Waze, imposter identities can negatively affect Google Maps by displaying false traffic congestion. In 2013, Tobias Jeske performed a man-in-the-middle attack on Google Maps, claiming that "attackers can anonymously manipulate the traffic analysis and actively influence the navigation of the software."[165] To prove his point, he drove a route in Hamburg, Germany and collected data packets sent to Google Maps from smartphones. To create traffic congestion on Google Maps, he took the intercepted smartphone data packets and re-sent them to the Google Maps server with modified indicators like time stamps, cookies, and platform keys. Figure 13 represents the Sybil attack via the man-in-the-middle method on a route in Hamburg, Germany. Multiple simulated vehicles were used to create traffic congestion on Google Maps.

Figure 13. Google Maps Man-in-the-Middle Attack[166]

[165] Jeske, "Floating Car Data from Smartphones," 12.

[166] Ibid.

3. Homeland Security Implications

The Sybil attacks on Waze and Google Maps demonstrate vulnerabilities that could lead to security concerns for surface transportation professionals and users. These vulnerabilities center on users' expectation of the apps' reliability and reputation. Waze is one of the most popular mobile navigation applications, with an estimated 50 million users as of 2013, the majority of whom commute in metropolitan areas.[167] In the San Francisco Bay Area, approximately 700,000 users implicitly trust Waze to guide their daily commutes.[168] Google Maps has a larger consumer base, with an average of one billion monthly users both online and through mobile applications.[169] Consumers act upon crowdsourced information almost instantaneously; between Waze and Google Maps, that is a large captive audience.[170] Waze and Google Maps users are also unlikely to back-check other traffic navigation sources—the crowdsourced information is not only manually input by users, but also by GPS transponders in mobile devices. Again, based on a sense of trust (implied by the terms of use) Waze and Google Maps users may be inclined to discount the possibility that information provided is false.

These vulnerabilities can allow a malicious actor to control and corral unwitting Waze and Google Maps users into gridlock. A gridlocked surface transportation system can paralyze a city's economy and standard of life. A paralyzed transportation system also presents a soft target for terrorist acts. As has been demonstrated, a malicious actor or group could set a "trap" by using a Sybil attack to suggest alternative routes based on false traffic congestion. The "trap" can be predetermined to maximize damage, both in human and infrastructure cost, through the use of vehicle-born explosives or suicide bombers.

---

[167] Peter Cohan, "Four Reasons Google Bought Waze," *Forbes*, June 11, 2013, http://www.forbes.com/sites/petercohan/2013/06/11/four-reasons-for-google-to-buy-waze/#2337dc3c1433.

[168] Jack Nicas, "Alphabet Unveils Program for Carpooling Via App Waze, Fraying Ties With Uber," *Wall Street Journal*, May 17, 2016, http://www.wsj.com/articles/alphabet-unveils-program-for-carpooling-via-app-fraying-ties-with-uber-1463428668.

[169] Ludovic Privat, "Google Maps: 1 Billion Monthly Users," *GPS Business News*, July 17, 2014, http://www.gpsbusinessnews.com/Google-Maps-1-Billion-Monthly-Users_a4964.html.

[170] Landon Cox, "Truth in Crowdsourcing," *IEEE Security and Privacy* 9, no. 5, (2011): 75.

The surface transportation system is a soft target with high potential for large-scale casualties.[171] Buses are the preeminent soft target for terrorist attacks, followed by trains, light rail, and their associated stations.[172] While highway infrastructure or passenger vehicles have not been popular terrorism targets, it seems inevitable that an attack will occur based on the history of terrorist attacks on public transportation—for instance, the 1995 Sarin Gas attack on the Tokyo subway system, the 2004 commuter rail bombings in Madrid, and the 2005 bombings of London buses.[173] A Sybil attack on Waze, Google Maps, or similar apps could provide a new target vector for terrorists, attracting them to highway infrastructure or passenger vehicles. This would be especially devastating in the United States, where the motor vehicle is the predominant mode of travel, with tens of millions of urban commuters daily.[174]

4. Social Navigation as Intelligence

So far, there has been no evidence of malicious actors using Waze or Google Maps as intelligence-gathering platforms to plan or orchestrate an attack. Previously in this thesis, a hypothetical scenario described how legitimate information on Twitter could be used to collect information and intelligence with which to orchestrate an attack. Like Twitter, Waze and Google Maps could be used to identify attack targets or to orchestrate an attack based on legitimate traffic congestion or traffic routing information.

Another Google product, however, Google Earth, has already been used by terrorist groups to launch attacks on British bases in Basra in 2013.[175] Lashkar-e-Taiba

---

171 Jenkins and Butterworth, *Troubling Trends*, 2.

172 Ibid., 2.

173 *Wikipedia*, s.v. "Tokyo Subway Sarin Attack," accessed July 14, 2016, https://en.wikipedia.org/wiki/Tokyo_subway_sarin_attack; Brian Michael Jenkins and Bruce R. Butterworth, *Long-Term Trends in Attacks on Public Surface Transportation in Europe and North America* (San Jose, CA: Mineta Transportation Institute, 2016), 2.

174 Tom Huddleston, Jr. "These U.S. Cities Have the Worst Commute Times," *Fortune*, March 3, 2016, http://fortune.com/2016/03/03/us-cities-average-commute-time/.

175 Thomas Harding, "Terrorists' Use of Google Maps to Hit UK Troops," *Telegraph*, January 13, 2007 http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html.

also used Google Earth to plan the 2008 Mumbai attacks.[176] While Google Earth is not a social navigation or traffic routing application, terrorists have demonstrated that Web 2.0 platforms are being used for intelligence purposes by terrorist organizations. It seems only a matter of time before Waze and Google Maps are used for similar purposes.

C. FUTURE CONCERNS

Though it is difficult to quantify how often malicious actors are using SMSN platforms, the data in Chapter IV and the analysis in this chapter infer that SMSN platforms can be exploited for information that will aid terrorist attacks. This poses a specific threat to surface transportation. Continued use of SMSN platforms in this manner should be anticipated because it is freely available; because of the sheer volume of users, it is difficult for security services to track information, and there is enough substantial information in SMSN to facilitate or enhance operational attack planning and execution.[177] This low risk of detection is perhaps the most compelling reason for malicious actors to continue using SMSN for intelligence gathering.[178]

Sybil attacks have been shown to exploit user trust by violating social navigation platforms' terms of use agreements. The potential of "weaponizing" a social navigation platform should be a growing concern for three reasons:

1. Sybil attacks are relatively cheap and "can be facilitated using free off-the-shelf emulation software, a simple fake GPS player application, running on a 16 core [computer] machine."[179]

2. Mobile app security breaches are rapidly increasing because apps have a minimal security framework when compared to traditional computer systems, and the number of users is growing dramatically.[180]

---

[176] John Ribeiro, "Google Earth Used by Terrorists in India Attacks," PCWorld, November 30, 2008, http://www.pcworld.com/article/154684/article.html.

[177] Eric Landree et al., *Assessing Publicly Available Data Regarding U.S. Transportation Infrastructure Security* (Santa Monica: RAND, 2007), 6.

[178] Ibid.

[179] Ben Sinai et al., *Exploiting Social Navigation*, 1.

[180] Bob Violino, "Mobile Apps the New Favorite for Hack Attack," CA Technologies, October 29, 2014, http://rewrite.ca.com/us/articles/security/mobile-apps-the-new-favorite-for-hack-attack.html.

3. Terrorist groups are improving their cyberattack capabilities. For example, ISIS has the hacking capability to launch "a major attack against government infrastructure," and Distributed Denial of Service attacks have been a favorite attack vector for the Syrian Electronic Army and OpIsreal against government cites.[181] Mobile applications provide a rich target environment for hacking activities.

Further research is needed in each of these potential areas of vulnerability.

[181] Pierluigi Paganini, "Ghost Security Group Has Reportedly Discovered an Android Mobile Application Used by Members of the ISIS Organization for Secure Communications," *Security Affairs*, December 7, 2015, http://securityaffairs.co/wordpress/42581/intelligence/isis-mobile-app.html; Gabi Siboni, Daniel Cohen, and Aviv Rotbart, "The Threat of Terrorist Organizations in Cyberspace," *Military and Security Affairs*, 5, no. 3 (December 2013): 21–22.

VI. CONCLUSION

At the beginning of this thesis, the question was asked: "What threats do social media and social navigation (SMSN) pose to the surface transportation system?" Early on, it was noted that current literature regarding SMSN does not assess the potential security threats these platforms pose to surface transportation. The intent of this thesis was to identify those vulnerabilities, catalog them, and provide context for how those vulnerabilities represent threats to surface transportation security.

A. SUMMARY OF FINDINGS

While available research and open-source information is somewhat limited, three research groups have successfully manipulated and exploited social navigation systems such as Waze and Google Maps. In two cases, both social media and social navigation platforms were used by terrorist organizations for attack planning and intelligence purposes. Academic researchers have been responsible for discovering vulnerabilities in Google Maps and Waze by utilizing various forms of Sybil attacks.

Waze and Google Maps provide real-time traffic information as well as navigational assistance to millions of commuters' worldwide. Users are dependent on the data and suggested routing choices to make their travel and commuting decisions. However, if malicious actors are able to perform Sybil attacks, they can lure motorists into potential "kill boxes" in the middle of a city. An attack of this nature could be economically destructive to infrastructure and, of course, devastating to human lives.

To date, malicious activities utilizing Sybil attacks on social media platforms have not been attributed to direct threats on surface transportation. Although there is no firm evidence that terrorist factions have considered this, known attributable threats have been aided by Google Earth mapping technologies and will almost certainly continue to provide intelligence as attack plans are constructed.[182] Significant data already identifies

[182] Harding, "Terrorists' Use of Google Maps"; Ribeiro, "Google Earth Used by Terrorists."

public transportation as soft targets.[183] The combination of surface transportation, applications that support mapping technologies, and the pervasive use of social media is a recipe for disaster. Such an attack is no longer simply a futurist consideration of fiction; it is a real and present danger. Web 2.0's fundamental intent is to provide access to shared information—this information cannot be controlled in the presence of malicious activities and is subject to monitor malintent.[184] Terrorist groups' increased capacity to exploit these platforms and to operate without suspicion is expected to rise.[185]

B. HOMELAND SECURITY RAMIFICATIONS

Society's reliance on technology has opened avenues for data collection that terrorist groups can manipulate. This app-reliance is based on ease of access and the consumer's trust that information is given without maleficence. Terrorist acts involve not only the collection and interpretation of data, but also the possibility of manipulated data intended to affect the consumer's choices.[186] For example, phishing attacks are still an effective mechanism to lure individuals into threatening emails.[187] In parallel, apps like Waze and Google Maps have the potential to be manipulated in order to lure a concentration of vehicle surface transportation to a point of attack for increased effect. SMSN applications can be used as weapons of destruction within surface transportation systems. Homeland security and transportation security professionals must be prepared to prevent or react to such an attack.

In assessing our nation's vulnerability to asymmetric attacks, the 9/11 Commission Report identified a "lack of imagination" within our security apparatus.[188] The notion that terrorists can manipulate social media and navigation applications to steer

---

183 Jenkins and Butterworth, *Troubling Trends*, 2.

184 Wu, "Impossible to Regulate," 286.

185 P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2013), 70.

186 Ibid

187 Danny Palmer, "Malicious Phising Attacks are Far More Effective than Most Businesses Realize, Claims Expert," *Computing*, November 20, 2014, http://www.computing.co.uk/ctg/news/2382628/malicious-phishing-attacks-are-far-more-effective-than-most-businesses-realise-claims-expert.

188 National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York, W. W. Norton, 2011), 346.

commuters into dense areas may be imaginative, but no more so than the 9/11 attacks on the World Trade Center and the Pentagon.[189] According to Presidential Policy Directive 21, transportation systems are viewed as a critical infrastructure sector.[190] Social navigation applications such as Waze and Google Maps influence the operations of transportation systems, and therefore consideration should now be given to labeling them, too, as critical elements of the surface transportation infrastructure, and they should be secured as such.

C. IMPLICATIONS FOR FUTURE RESEARCH

Many view autonomous vehicles as the solution to America's traffic congestion problems.[191] Ride-sharing company Lyft is attempting to create a new market by partnering with General Motors to develop a network of autonomous ride-sharing vehicles (see Figure 14).[192]

[189] Ibid.

[190] "Presidential Policy Directive—Critical Infrastructure Security and Resilience," The White House, February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[191] Earl Blumenauer, "Let's Use Self-Driving Cars to Fix America's Busted Infrastructure," *Wired*, May 20, 2016, https://www.wired.com/2016/05/lets-use-self-driving-cars-fix-americas-busted-infrastructure/.

[192] Alex Davies, "GM and Lyft Are Building a Network of Self-Driving Cars," *Wired*, January 4, 2016, https://www.wired.com/2016/01/gm-and-lyft-are-building-a-network-of-self-driving-cars/.

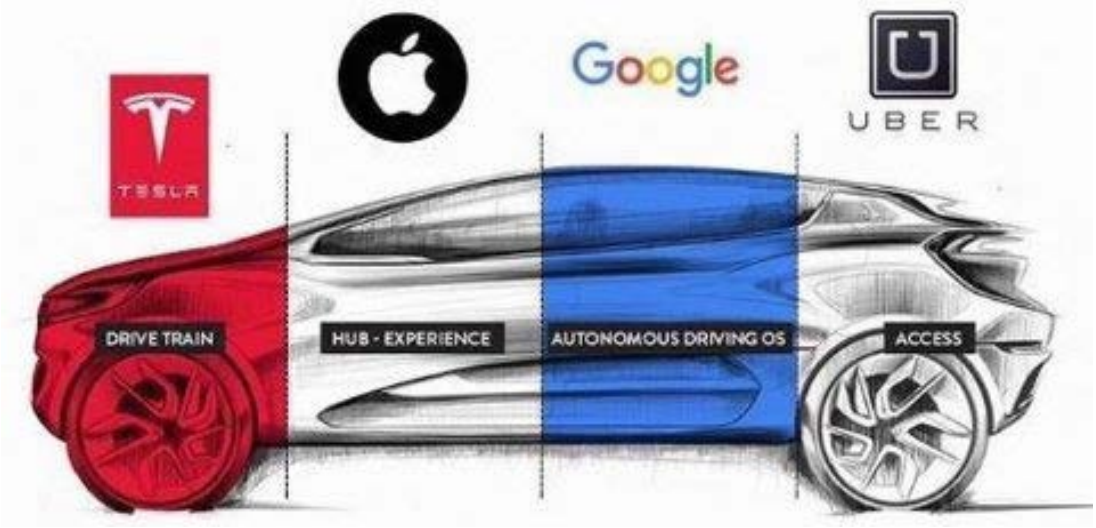


Figure 14. Web 2.0 in Autonomous Vehicles[193]

The upcoming wave of autonomous vehicles will certainly have a positive effect on surface transportation.[194] However, understanding the importance of vehicle surface transportation security and identifying vulnerabilities in the implementation of autonomous vehicles should be considered as well. As has been demonstrated, SMSN applications and algorithms will impose their vulnerabilities upon autonomous vehicles, which have the potential to be used as controlled weaponized devices. Hypothetically, Sybil attacks could directly influence multiple autonomous vehicles to perform the bidding of terrorists and criminals (see Figure 15).[195]

[193] Nunzio Presta, "What Does the Autonomous Car Mean to the World!" LinkedIn, October 29, 2015, https://www.linkedin.com/pulse/what-does-autonomous-car-mean-world-nunzio-presta.

[194] Jack Stewart, "People Want Self-Driving Cars That Save Lives. Especially Theirs," *Wired*, June 23, 2016, https://www.wired.com/2016/06/people-want-self-driving-cars-save-lives-especially/.

[195] Rupesh Gunturu, "Survey of Sybil Attacks in Social Networks," Cornell University Library, accessed April 15, 2016, http://arxiv.org/pdf/1504.05522v1.pdf.

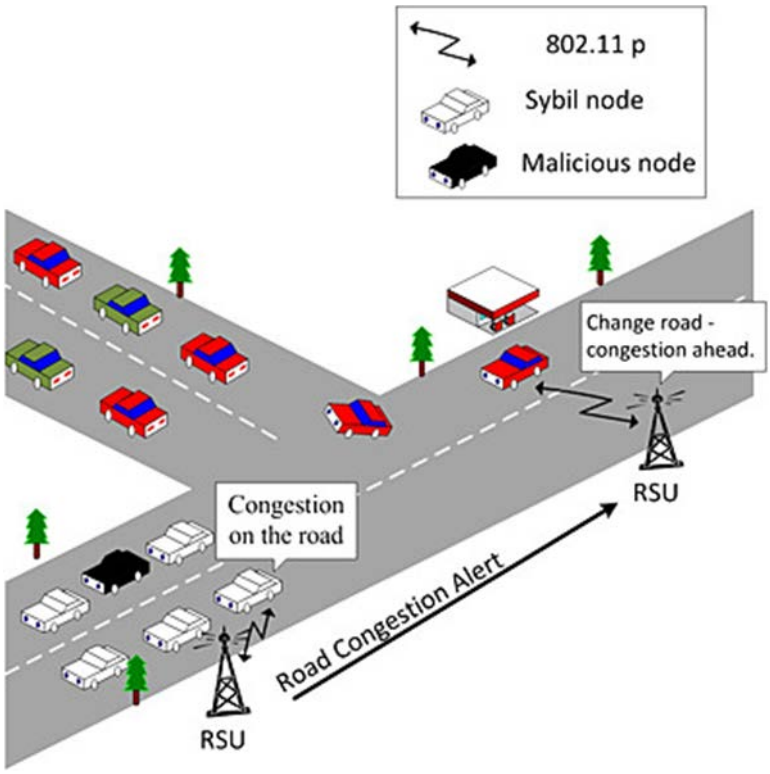


Figure 15. Sybil Attack in a Vehicle Area Network[196]

Lastly, autonomous vehicles are expected to communicate with transportation infrastructure to ensure efficient and safe traffic flow.[197] Vehicles are anticipated to convey lane positioning, travel speed, and distance to traffic signals; in turn, traffic signals can adjust signal timing to accommodate approaching vehicles to make traffic flow more efficient (see Figure 16).[198] A Sybil attack or a man-in-the-middle attack on the traffic infrastructure and/or vehicular network could cause vehicle conflicts and accidents at intersections by communicating false vehicle characteristic information and false traffic infrastructure information. Further research is required to explore security

[196] Khaled Rabieh, Mohamed Mahmoud, Marianne Azer, and Mahmoud Allam, "A Secure and Privacy-Preserving Event Reporting Scheme for Vehicular Ad Hoc Networks: Security in Event Reporting Scheme," *Security and Communication Networks* 8, no. 17 (March 2014): Figure 2, https://www.researchgate.net/figure/274731284_fig6_Figure-2-Sybil-attack-scenario-RSU-road-side-unit.

[197] "Vehicle-to-Infrastructure (V2I) Communications for Safety," U.S. Department of Transportation, accessed July 12, 2016, http://www.its.dot.gov/factsheets/v2isafety_factsheet.htm.

[198] This is based on my experience as a traffic and transportation engineer.

counter-measures that could deny malign exploitation of the booming autonomous vehicle industry.

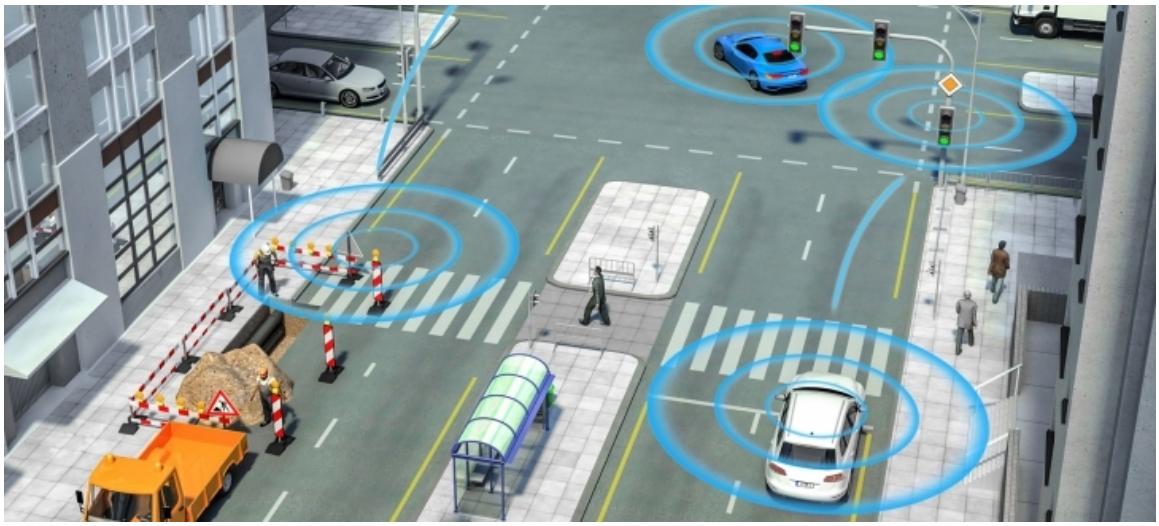


Figure 16. Vehicle-to-Infrastructure Communication[199]

D. FINAL REMARKS

The present and future protection of transportation infrastructure has room for improvement and will require imagination to outsmart malicious actors working diligently to find holes within our systems. The threats posed to vehicle surface transportation by vulnerabilities in Web 2.0 have been explored through the lens of cyber security, vehicle surface transportation security, and social media exploitation. Vulnerabilities to social media and navigation applications have been identified and categorized. These vulnerabilities must now be addressed by homeland security, transportation, and information technology professionals.

[199] "Connected Vehicles," Metropolitan Transportation Commission, accessed August 14, 2016, http://mtc.ca.gov/our-work/operate-coordinate/intelligent-transportation-systems/connected-vehicles-0.

LIST OF REFERENCES

Agarwal, Nitin, Shamanth Kumar, Huji Gao, Reza Zafarani, and Huan Liu. "Analyzing Behavior of the Influentials Across Social Media." In *Behavior Computing: Modeling Analysis, Mining and Decision*, edited by Longbing Cao and Philip S. Yu, 3–19. New York: Springer: 2012.

Amble, John Curtis. "Combating Terrorism in the New Media Environment." *Studies in Conflict & Terrorism*, 35, no. 5, (2012): 339–353. doi: 10.1080/1057610X.2012.666819.

Apatu, Emma, Melissa Alperin, Kathleen Miner, and David Wiljer. "A Drive through Web 2.0—An Exploration of Driving Safety Promotion on Facebook." *Health Promotion Practice* 14, no. 1 (January 2013): 88–95.

Barabasi, Albert-Laszlo. *Linked—How Everything Is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*. New York: Plume-Penguin Group, 2002.

Barlas, Stephen, Alan Earls, Michael Fitzgerald, Jerri Ledford, and Dennis McCafferty. "U.S. Critical Infrastructure Security: Highlighting Critical Infrastructure Threats." TechTarget. Accessed March 3, 2016. http://searchsecurity.techtarget.com/US-critical-infrastructure-security-Highlighting-critcal-infrastructure-threats.

Ben Sinai, Meital, Nimrod Partush, Shir Yadid, and Eran Yahav. *Exploiting Social Navigation*. Haifa, Israel: The Technion, 2014.

Boulos, Maged Kamel, Antonio Sanfilippo, Courtney Corley, and Steve Wheeler. "Social Web Mining and Exploitation for Serious Applications: Technosocial Predictive Analytics and Related Technologies for Public Health, Environmental and National security Surveillance." *Computer Methods and Programs in Biomedicine* 100, no. 1 (October 2010): 16–23. doi: 10.1016/j.cmpb.2010.02.007.

California Department of Transportation. "Caltrans Partners with Waze Connected Citizens Program," April 5, 2016. http://www.dot.ca.gov/paffairs/pr/2016/prs/16pr033.html.

Cavalini, Matteo, and John Austen. *Terrorist Use of the internet*. Egham, UK: Royal Holloway, 2014.

Chamales, George. *Towards Trustworthy Social Media and Crowdsourcing*. Washington, DC: Wilson Center, 2013.

Cheong, France, and Christopher Cheong. "Social Media Data Mining: A Social Network Analysis of Tweets during the 2010–2011 Australian Floods." Paper presented at the Pacific Asian Conference on Information Systems, Brisbane, Australia, July 7–11, 2011.

Cox, Landon. "Truth in Crowdsourcing." *IEEE Security and Privacy* 9, no. 5, (2011): 74–76.

"Crowdsourced Traffic Apps: Saving Commuters from Traffic Jam Torture." *Scratch*, February 10, 2015. http://www.scratchmarketing.com/crowdsourced-traffic-apps/.

Dahl, Dick. "Experts Explore How Social Networks Can Influence Behavior and Decision Making." Video. Harvard Law School, February 15, 2013. http://today.law.harvard.edu/experts-explore-how-social-networks-can-influence-behavior-and-decision-making-video/.

Dror, Talia, Sagi Dalyot, and Yerach Doysther. "A Quantitative Geo-Evaluation of Crowdsourcing and Wisdom of the Crowd." International Federation of Surveyors, December 2014. http://www.fig.net/resources/monthly_articles/2014/december_2014/december_2014.pdf.

Drozdova, Katya, and Michael Samoilov. "Predictive Analysis of Concealed Social Network Activities Based on Communication Technology Choices: Early-Warning Detection of Attack Signals from Terrorist Organizations." *Computational and Mathematical Organization Theory* 16, no. 1 (March 2009): 61–88.

Everton, Sean F. *Disrupting Dark Networks*. New York: Cambridge University Press, 2011.

Federman Josef, and Max J. Rosenthal. "Waze Sale Signals New Growth for Israeli High Tech." Yahoo, June 12, 2013. https://www.yahoo.com/news/waze-sale-signals-growth-israeli-high-tech-174533585.html?ref=gs.

Freeman, Gregory, and Robert Schroeder. *Social Media Exploitation: An Assessment*. Monterey, CA: Naval Postgraduate School, 2014.

Frey, Davide, Arnaud J´egou, and Anne-Marie Kermarrec. "Social Market: Combining Explicit and Implicit Social Networks." Paper presented at the International Symposium on Stabilization, Safety, and Security of Distributed Systems, Grenoble, France, October 2011.

Fu, Kaiquan, Chang-tien Lu, Rakesh Nune, and Jason Tao. "Steds: Social Media based Transportation Event Detection with Text Summarization." Paper presented at the 2015 IEEE 18th International Conference on Intelligent Transportation Systems, Canary Islands, Spain, September 15–18, 2015.

Georgiou, Theodore, Amr El Abbadi, Xifeng Yan, and Jemim George. *Mining Complaints for Traffic Jam Estimation: A Social Sensor Application*. Santa Barbara: University of California Santa Barbara, 2015.

Goodman, Marc. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do about it.* New York: Knopf Doubleday, 2014.

Google. "Google Maps/Google Earth Additional Terms of Service." December 17, 2015, https://www.google.com/intl/ALL/help/terms_maps.html.

Goolsby, Rebecca. *On Cybersecurity, Crowdsourcing, and Social Cyber-Attack.* Washington, DC: Wilson Center, 2013.

Greenway, David. "Students Fake a Traffic Jam in Waze to Clear Their Route." htxt.africa. Accessed July 8, 2015. http://www.htxt.co.za/2014/03/26/students-fake-a-traffic-jam-in-waze-to-clear-their-route/.

Gunturu, Rupesh. "Survey of Sybil Attacks in Social Networks." Cornell University Library. Accessed April 15, 2016. http://arxiv.org/pdf/1504.05522v1.pdf.

Jenkins, Brian Michael and Bruce R. Butterworth. *Long-Term Trends in Attacks on Public Surface Transportation in Europe and North America*. San Jose, CA: Mineta Transportation Institute, 2016.

———. *Troubling Trends in Terrorism and Attacks on Surface Transportation: The Outlook is Grim, but People Still Have a Great Deal of Control*. San Jose, CA: Mineta Transportation Institute, 2015.

Hickson, Alan. *Terrorist Threat to U.S. Highway Systems*. Washington, DC: Department of Homeland Security, Transportation Security Administration, 2006.

Howard, Alexander. "What is a Sybil Attack." TopTen Reviews, August 2, 2011. http://anti-virus-software-review.toptenreviews.com/what-is-a-sybil-attack-.html.

Ibrahim, Saleh, Reda Ammar, Sanguthevar Rajaskaran, Nicholas Lownes, Qixing Wang, and Dolly Sharma. "An Efficient Heuristic for Estimating Transportation Network Vulnerability." *2011 IEEE Symposium on Computers and Communications (ISCC)*: 1092–1098.

INFOSEC Institute. "The Role of Technology in Modern Terrorism." February 3, 2016. http://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/.

Jeske, Tobias. "Floating Car Data from Smartphones—What Google and Waze Know about You and How Hackers Can Control Traffic." Paper presented at Black Hat Europe, Amsterdam, March 12–15, 2013.

Kongthon, Alisa, Choochart Harechaiyasak, Jaruwat Pailai, and Sarawoot Kongyoung. "The Role of Twitter during a Natural Disaster: A Case Study of the 2011 Thai Food." Paper presented at PICMET '12: Technology Management for Emerging Technologies, Vancouver, British Columbia, July 29–August 2, 2012).

Kocetepe, Aybek. Javier Lores, Eren Erman Ozguven, and Anil Yazici. "The Reach and Influence of DOT Twitter Accounts: A Case Study in Florida." Paper presented at the 18th International Conference on Intelligent Transportation Systems, Canary Islands, Spain, September 15–18, 2015.

Landree, Eric, Christopher Paul, Beth Grill, Aruna Balakrishnan, Bradley Wilson, and Martin Libicki. *Assessing Publicly Available Data Regarding U.S. Transportation Infrastructure Security*. Santa Monica: RAND, 2007.

Laskey, Kathryn Blackmond. "Crowdsourced Decision Response for Emergency Responders." Paper presented at the 18th International Command and Control Research & Technology Symposium, Alexandria, VA, June 19–21, 2013.

Lindsay, Bruce R. *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations* (CRS Report No. R41987). Washington, DC: Congressional Research Service, 2011.

Metropolitan Transportation Commission. "Connected Vehicles." Accessed August 14, 2016. http://mtc.ca.gov/our-work/operate-coordinate/intelligent-transportation-systems/connected-vehicles-0.

Murray-Tuite, Pamela**,** and Xiang Fe. "A Methodology for Assessing Transportation Network Terrorism Risk with Attacker-Defender Interactions." *Computer-Aided Civil Engineering* 25, no. 6 (August 2010): 396–410.

National Commission on Terrorist Attacks. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* New York, W. W. Norton, 2011.

Oh, Onook, Manish Agrawal, and H. Raghav Rao. "Information Control and Terrorism: Tracking the Mumbai terrorist Attack through Twitter." *Information Systems Front* 13, no. 1 (March 2011): 33–43.

Olanoff, Drew. "Deep Dive with the New Google Maps for Desktop with Google Earth Integration, It's More than Just a Utility." Tech Crunch, May 15, 2013. https://techcrunch.com/2013/05/15/deep-dive-with-the-new-google-maps-for-desktop-with-google-earth-integration-its-more-than-just-a-utility/.

Perez, Sarah. "Navigation App Waze Gets a Huge Redesign-Now Less Cluttered, but Still Needs Improvement." Tech Crunch, last modified October 19, 2015. http://techcrunch.com/2015/10/19/navigation-app-waze-gets-a-huge-redesign-now-less-cluttered-but-still-needs-improvement/#.zpel8b:KuBe.

Presta, Nunzio. “What Does the Autonomous Car Mean to the World!” LinkedIn, October 29, 2015. https://www.linkedin.com/pulse/what-does-autonomous-car-mean-world-nunzio-presta.

Raab, Jorg, and H. Brinton Milward. “Dark Networks as Problems.” *Journal of Public Administration Research and Theory* 13, no. 4, (2003): 413–439, doi: 10.1029/jopart/mug029.

Rabieh, Khaled, Mohamed Mahmoud, Marianne Azer, and Mahmoud Allam. “A Secure and Privacy-Preserving Event Reporting Scheme for Vehicular Ad Hoc Networks: Security in Event Reporting Scheme,” *Security and Communication Networks* 8, no. 17 (March 2014). https://www.researchgate.net/figure/274731284_fig6_Figure-2-Sybil-attack-scenario-RSU-road-side-unit.

Raphiphan, Panraphee, Arkady Zaslasky, and Maria Indrawan-Santiago. “Building Knowledge from Social Networks on What Is Important to Drivers in Constrained Road Infrastructure.” Paper presented at the 18th International Conference on Knowledge Based and Intelligent Information & Engineering Systems, Gydnia, Poland, 2014.

Rebelo, Francisco, Carlos Soares, and Rosaldo Resetti. “TwitterJam: Identification of Mobility Patterns in Urban Centers based on Tweets.” Paper presented at the 2015 IEEE First International Smart Cities Conference (ISC2), Guadalajara, Mexico, October 25–28.

Ribeiro, John. “Google Earth Used by Terrorists in India Attacks.” PCWorld, November 30, 2008. http://www.pcworld.com/article/154684/article.html.

Ribeiro, Silvio, Diogo Renno Oliveira, Tatiana Goncalves, Clodoveu Davis Jr., Wanger Meira Jr., and Gisele Pappa. “Traffic Observatory: A System to Detect and Locate Traffic Events and Conditions Using Twitter.” Paper presented at the 5th ACM Sigspatial International Workshop on Location Based Networks, Redondo Beach, CA, November 6, 2012.

Sakai, Takeshi, Fujio Toriumi, Koki Uchiyama, Yutaka Matsuo, Kosuke Shinoda, Kazuhiro Kazama, Soshi Kurihara, and Itsuki Noda. “The Possibility of Social Media Analysis for Disaster Management.” Paper presented at the 2013 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Sendai, Japan, August 26–29, 2013.

Saperstone, Max. “Using Genymotion to Simulate a Moving Device.” coveros, November 10, 2015. https://www.coveros.com/using-genymotion-to-simulate-a-moving-device/.

Schneider, Nathan K. *ISIS and Social Media—The Combatant Commander’s Guide to Countering ISIS’s Social Media Campaign*. Newport, RI: Naval War College, 2015.

Siboni, Gabi, Daniel Cohen, and Aviv Rotbart. “The Threat of Terrorist Organizations in Cyberspace.” *Military and Security Affairs*, 5, no. 3 (December 2013): 3–29.

Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2013.

Stieglitz, Stefan, and Linh Dang-Xuan. “Emotions and Information Diffusion in Social-Media—Sentiment of Microblogs and Sharing Behavior.” *Journal of Management Information Systems* 29, no. 4, (April 2013): 217–248.

TeskaLabs. “What Is Man-in-the-Middle and How to Protect Your Data and Mobile Apps from Such Attacks.” Accessed August 14, 2016. https://www.teskalabs.com/blog/protect-mobile-app-and-prevent-man-in-the-middle-attack.

Transit Cooperative Research Program. *Use of Social Media in Public Transportation—A Synthesis of Transit Practice*. Washington, DC: Transportation Research Board, 2012. http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_syn_99.pdf.

Theohary, Catherine A., and John Rollins. *Terrorist Use of the internet: Information Operations in Cyberspace* (CRS Report No. R41674). Washington, DC: Congressional Research Service, 2011.

Trowbridge, Alexander. “ISIS Swiping Hashtags as Part of Propaganda Efforts.” CBSNews, August 26, 2014.http://www.cbsnews.com/news/isis-hijacks-unrelated-hashtags-in-attempt-to-spread-message/.

Underleider, Neal. “Waze Is Driving into City Hall.” Fast Company, last modified April 15, 2015. http://www.fastcompany.com/3045080/waze-is-driving-into-city-hall.

U.S. Department of Transportation. “Vehicle-to-Infrastructure (V2I) Communications for Safety.” Accessed July 12, 2016, http://www.its.dot.gov/factsheets/v2isafety_factsheet.htm.

Violino, Bob. “Mobile Apps the New Favorite for Hack Attack.” CA Technologies, October 29, 2014. http://rewrite.ca.com/us/articles/security/mobile-apps-the-new-favorite-for-hack-attack.html.

Wang, Gang, Bolun Wang, Tianyi Wang, Ana Nika, Bingzhe Liu, Haitao Zheng, and Ben Y. Zhao. “Defending against Sybil Devices in Crowdsourced Mapping Services.” Paper presented at MobiSys ‘16, Singapore, June 25–30, 2016.

Waze. “Terms of Use.” Accessed July 14, 2016. https://www.waze.com/legal/tos.

Weimann, Gabriel. *New Terrorism and New Media.* Washington, DC: Wilson Center, 2014.

The White House. “Presidential Policy Directive—Critical Infrastructure Security and Resilience.” February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Wiki Waze. “Your Rank and Points.” Accessed June 14, 2016. https://wiki.waze.com/wiki/Your_Rank_and_Points#Waze_Points_Level_.28in_client_app.29.

Wu, Paulina. “Impossible to Regulate: Social Media, Terrorists and a Role for the U.N..” *Chicago Journal of International Law* 16, no.1, (2015): 281–311.

Zohar, Shaul. “Report / Users / WAZE / 2013 / United States, Europe, Asia & Latin America.” Graphic, Evolita, September 18, 2014. http://alpha.evolita.com/Research/Subject/WAZE-Users-Europe-Asia-Latin-America-United-States-Y2013.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California